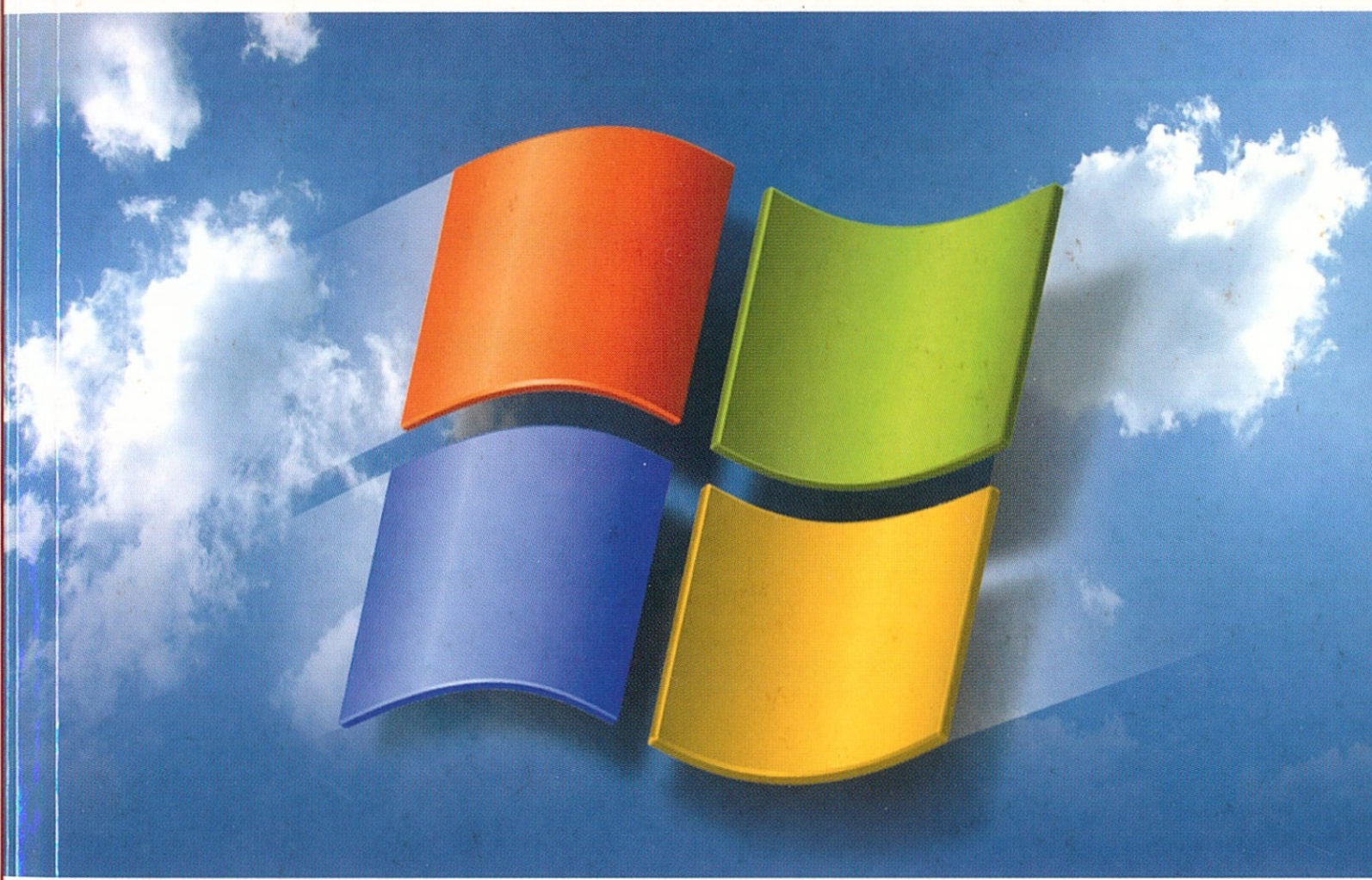
Windows XP Service Pack 2

haladóknak



CHIP

Professzionális

Windows XP Service Pack 2

haladóknak

CHIP

© 2004 VogelBurda Communication Kft., 1088 Budapest, Rákóczi út 1–3.
Felelős kiadó: Carsten Gerlach ügyvezető igazgató
Szerkesztő: Bányai Ferenc
Tervezőszerkesztő: Dancs Katalin
Címlapterv: Szincsák László

Minden jog fenntartva. Jelen könyvet, illetve annak részeit tilos reprodukálni, adatrendszerben tárolni, bármely formában vagy eszközzel – elektronikus, fényképészeti úton vagy más módon – a kiadó engedélye nélkül közölni.

A kötetet készítette:
Levilágítás: HVG Press
Nyomtatta és kötötte a Kaposvári Nyomda Kft. – 241265
Felelős vezető: Pogány Zoltán igazgató
ISBN 963 217 091 1
ISSN 1786-2825

TARTALOM

1 A Microsoft Windows XP 2. szervizcsomagja 5

A számítógépek által nyújtott szolgáltatások rohamosan bővülnek és fejlődnek. Ezzel párhuzamosan a vírusok, a férgek és a hackerek személyében újabb és újabb fenyegetések jelennek meg. A Microsoft ezért tulajdonít elsődleges fontosságot a biztonsági kérdéseknek, és segít a felhasználóknak megelőző módszerekkel megvédeni a számítógépet, az információt és a személyes adatokat.

2 Technológiai áttekintés 13

A Microsoft Windows XP továbbfejlesztett biztonsági technológiákat tartalmazó 2. szervizcsomagja bővített biztonsági infrastruktúrát kínál a felhasználóknak a vírusok, férgek és behatolók elleni hatékony védelemhez.

3 Telepítés és használat 26

Ez a fejezet lépésről-lépésre haladva mutatja be a telepítés menetét, valamint egyszerű útmutatásokat kínál a továbbfejlesztett biztonsági technológiák használatának megkönnyítésére.

4 Az SP2 optimális telepítése 45

Ebben a fejezetben ismét a telepítés áll a középpontban: bemutatjuk azokat a módszereket és beállításokat, amelyekkel az egyéni felhasználók a legoptimálisabb módon telepíthetik az SP2-t.

5 Az SP2 integrálása az XP telepítőlemezébe 56

Kevesen tudnak róla, de az SP2-t úgy is beágyazhatjuk az XP operációs rendszerbe, hogy létrehozunk egy új, SP2-vel kiegészített XP telepítőlemezt. Ennek előnyeit talán felesleges is ecsetelni: azzal ugyanis, hogy már telepítéskor ott vannak a javítások a rendszerben, nagy súly kerül le a vállunkról.

6 Windows kontra Linux 62

Sokan állítják, hogy a Linux biztonságosabb, mint a Windows. Ebben a fejezetben ennek az állításnak járunk utána.

7 12 kérdés a 2. szervizcsomagról 74

A Microsoft most minden idők „legméretesebb" Windows-frissítését kínálja. Valóban megéri-e telepíteni ezt az óriáscsomagot? Ebben a fejezetben a 12 legégetőbb kérdésre keressük a választ a szervizcsomaggal kapcsolatban.

8 Problémák az XPSP2-vel 82

Bár az XP Service Pack 2 kétségtelenül jelentős előrelépés a biztonság terén, és remélhetőleg ahhoz is hozzájárul, hogy az internet egészében biztonságosabb „hely" legyen, nem hunyhatjuk be a szemünket a vele kapcsolatos problémák felett sem. Ez a fejezet ezekről a problémákról ad számot.

9 A 2. szervizcsomag üzleti értéke 87

Ez a fejezet azt ismerteti, hogy a Windows XP alapú számítógépeken miként tehető hatékonyabbá és könnyebbé a vállalati adatok védelme és a biztonsági szolgáltatások kezelése, és miként biztosítható a felhasználók produktivitása a 2. szervizcsomag telepítésével.

1 A Microsoft Windows XP 2. szervizcsomagja

A számítógépek által nyújtott szolgáltatások rohamosan bővülnek és fejlődnek. Ezzel párhuzamosan a vírusok, a férgek és a hackerek személyében újabb és újabb fenyegetések jelennek meg. A Microsoft ezért tulajdonít elsődleges fontosságot a biztonsági kérdéseknek, és segít a felhasználóknak megelőző módszerekkel megvédeni a számítógépet, az információt és a személyes adatokat.

A Microsoft Windows XP 2. szervizcsomagja *(XP SP2)* továbbfejlesztett biztonsági technológiákat kínál. A szervizcsomag kényelmesen kezelhető, egy helyre összegyűjtött, naprakész illesztőprogramokat és segédeszközöket, valamint biztonsági kiegészítéseket és egyéb létfontosságú frissítéseket tartalmaz. A Windows XP legújabb, elsősorban biztonsági javításokat és fejlesztéseket tartalmazó szervizcsomagja – a 2. szervizcsomag – a valaha kiadott legfontosabb szervizcsomagok közé tartozik.

1.1 Új szolgáltatások

A frissítések, újítások és továbbfejlesztett biztonsági technológiák átfogó gyűjteményét tartalmazó 2. szervizcsomag több új szolgáltatást is nyújt. A nem kívánt tartalom és letöltések kiküszöbölésére szolgáló új technológiák kényelmesebb internetes böngészést és kommunikációt tesznek lehetővé.

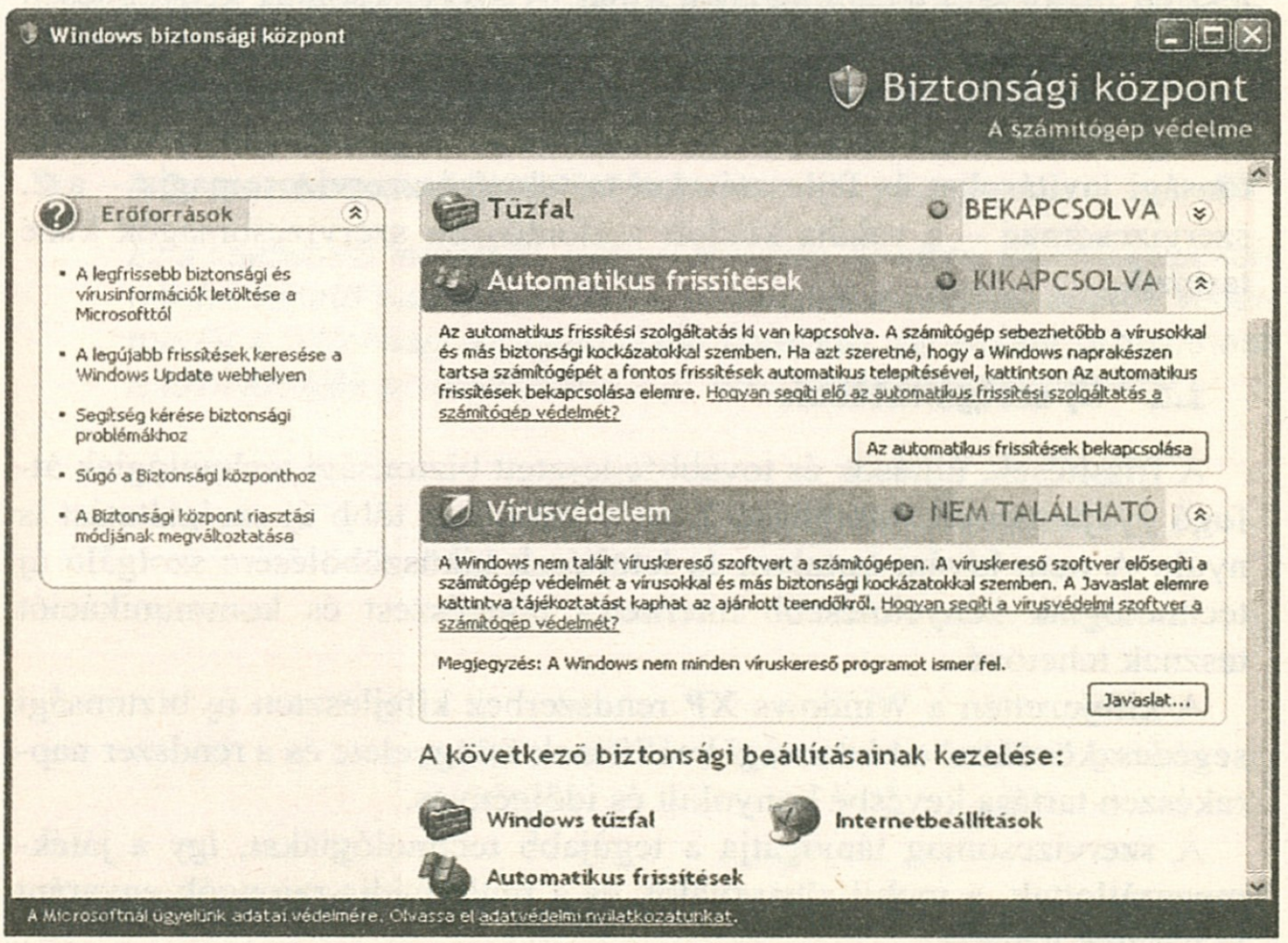
A kifejezetten a Windows XP rendszerhez kifejlesztett új biztonsági segédeszközökkel a biztonsági beállítások felügyelete és a rendszer naprakészen tartása kevésbé bonyolult és időigényes.

A szervizcsomag támogatja a legújabb technológiákat, így a játékmegszállottak, a mobilfelhasználók és a multimédia-rajongók egyaránt jó hasznát vehetik.

1.2 A biztonság eszközei

A 2. szervizcsomagnak a Windows XP rendszerű számítógépre való telepítése után biztosak lehetünk abban, hogy a számítógépen ettől kezdve a lehető legbiztonságosabb Windows operációs rendszer fut. A rendelkezésre álló új szolgáltatások és az alapértelmezett biztonsági óvintézkedések minden szinten lényegesen javítják a biztonságot. Nézzünk erre néhány példát.

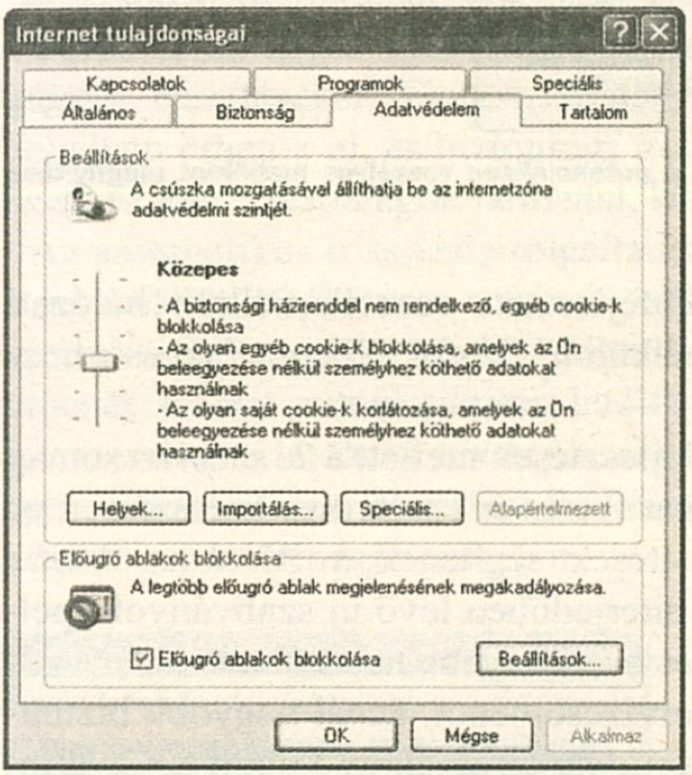
A *Windows Biztonsági központ* segítségével kézben tarthatjuk a biztonsági beállításokat. Az új Windows Biztonsági központ a Windows XP biztonsági beállításainak felügyeletére szolgáló új központi eszköz. Segítségével egyetlen szempillantás alatt felmérhető a számítógép védettségének aktuális szintje, egyebek között a tűzfal állapota, az automatikus frissítési beállítások és a vírusvédelem.



Biztonsági központ: rajta keresztül központilag szabályozható az új tűzfal, az automatikus frissítések és a vírusvédelem

A *Windows tűzfal* elősegíti a számítógép védelmét. Az alapértelmezés szerint bekapcsolt új, beépített Windows tűzfal segít megvédeni a számítógépet az interneten keresztül érkező vírusoktól és különféle behatolóktól.

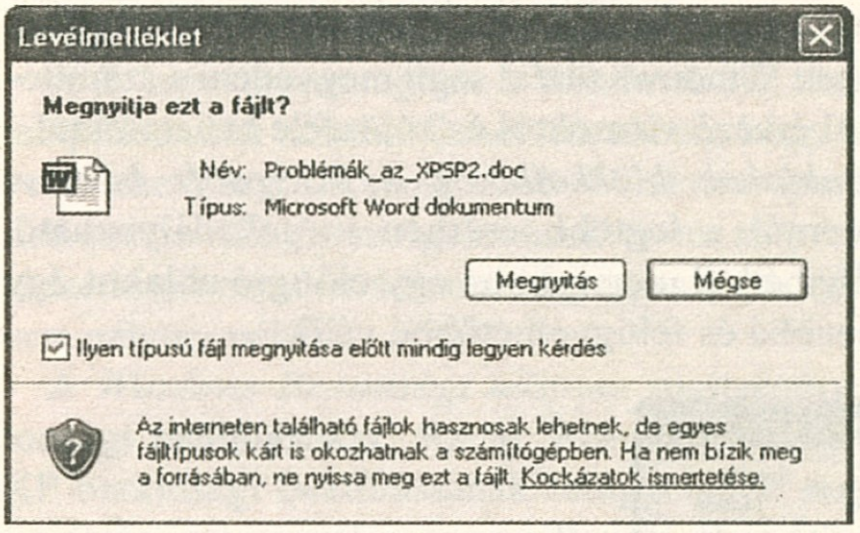
A bosszantó *előugró ablakok blokkolhatók* a *Microsoft Internet Explorer* programban. Ezentúl a legtöbb esetben megakadályozható, hogy egy webhely engedély nélkül megnyisson egy előugró ablakot, így a webböngészés zavartalanabbá és felügyelhetőbbé válik.



Új funkció az előugró ablakok blokkolásának lehetősége

Az *Outlook Express* program javításainak köszönhetően elkerülhető a kártékony kommunikáció. Az e-mail üzenetekkel olyan mellékletek is érkezhetnek, amelyek pusztító vírusokat tartalmaznak. Az Outlook Express új *mellékletkezelője* megnyitáskor elszigeteli a mellékleteket a számítógép többi részétől, s ezzel megakadályozza a veszélyes mellékletek megnyitását, amelyek esetleg vírusokkal vagy férgekkel fertőznék meg a rendszert.

Még biztonságosabban használhatók a *vezeték nélküli hálózatok.* Ha vezeték nélküli hálózatot üzemeltetünk, vagy laptop számítógépünkkel internetkávézóban vagy repülőtéren kapcsolódunk az internethez, a 2.



A Outlook Express kérdést szegez nekünk a potenciálisan veszélyes melléklet megnyitása előtt

szervizcsomagban szereplő továbbfejlesztett vezeték nélküli hálózati funkciók egyszerűsítik a vezeték nélküli hálózatok felismerését és a hozzájuk való csatlakozást.

A figyelemre méltó biztonsági fejlesztések mellett a 2. szervizcsomag tartalmazza a Microsoft legújabb hardveres és szoftveres fejlesztéseit is. Az új illesztőprogramok és frissítések segítenek a *Windows Media Player,* a *Microsoft DirectX* és az elterjedőben levő új szabványok (például a *Bluetooth)* biztonságosabb és hatékonyabb használatában.

Minél hamarabb telepítjük a szervizcsomagot, annál nagyobb biztonságban érezhetjük magunkat. Itt az ideje tehát, hogy telepítsük a Windows XP operációs rendszert erősebbé és biztonságosabbá tevő ingyenes 2. szervizcsomagot. A szervizcsomag – ingyenes – letöltéséhez keressük fel a **www.microsoft.com/hun/protect** webhelyet. Ezzel a lépéssel gyakorlatilag mindent megtettünk a számítógép és a rajta tárolt értékes személyes adatok védelme érdekében.

Rendszerkövetelmények

A 2. szervizcsomag telepítéséhez Microsoft Windows XP operációs rendszerrel működő személyi számítógép szükséges, amelyben van CD-meghajtó, 233 MHz-es vagy nagyobb órajel-frekvenciájú processzor, legalább 64 Mbájt RAM memória és a telepítés idejére legalább 900 Mbájt szabad merevlemez-terület.

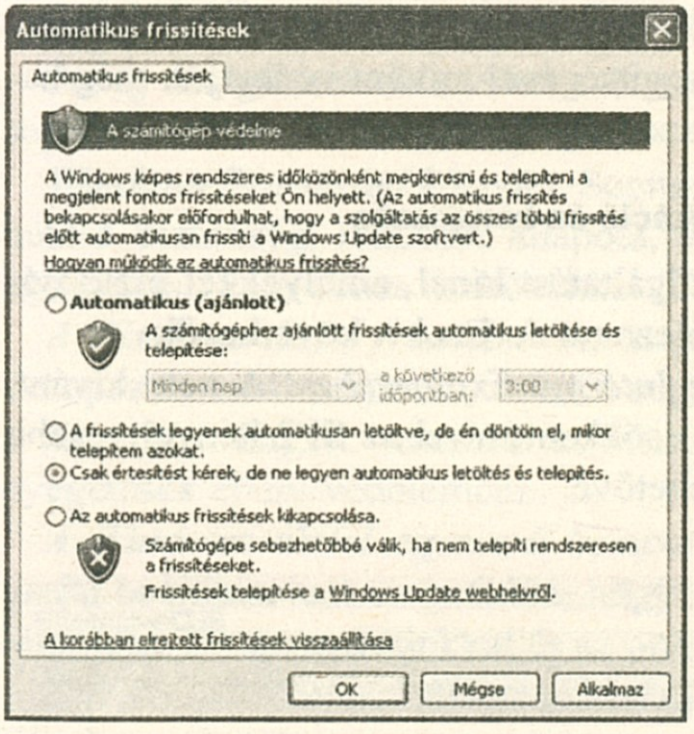
Tipp
A számítógép naprakészen tartását bízzuk a Windows XP *automatikus frissítési* funkciójára.

TiPP PLUSZ

1.3 Automatikus frissítés

A Windows *automatikus frissítési* szolgáltatása rendszeresen ellenőrzi a vírusok és az egyéb biztonsági fenyegetések elleni védelmet szolgáló legújabb frissítéseket. Ezek a fontos frissítések a *Windows Update* webhelyen érhetők el, és biztonsági frissítések, kiemelt fontosságú frissítések és szervizcsomagok tartoznak közéjük.

Az automatikus frissítési szolgáltatás bekapcsolása után nem szükséges egyenként megkeresni a frissítéseket az interneten, vagy a hiányzó javítások miatt aggódni. A Windows a felhasználó által meghatározott ütemezés szerint automatikusan letölti és telepíti ezeket. Ha saját magunk szeretnénk letölteni és telepíteni a frissítéseket, akkor beállíthatjuk, hogy az *Automatikus frissítések* funkció figyelmeztessen a kiemelt jelentőségű frissítések megjelenésekor.



Automatikus fissítések: szabadon szabályozhatjuk, hogyan menedzselje a Windows a frissítéseket

Kapcsoljuk be az *Automatikus frissítések* funkciót. Ez a legegyszerűbb módszer a megjelenő frissítések és javítások által nyújtott előnyök lehető leggyorsabb kihasználására.

Az Automatikus frissítések funkció egyszerűen beállítható:

Kattintsunk a *Start* gombra, válasszuk a *Vezérlőpult* parancsot, majd kattintsunk a *Teljesítmény és karbantartás,* és végül a *Rendszer* elemre. Váltsunk az *Automatikus frissítések* lapra, és jelöljük be a *Töltse le a frissítéseket automatikusan, és a megadott ütemezés szerint telepítse őket* választókapcsolót. Jelöljük ki, hogy melyik napon és mikor szeretnénk letölteni és telepíteni a frissítéseket.

Megjegyzés

Sokan emlékezhetnek rá, hogy 2003 augusztusában megjelent a Microsoft Windows XP 1. szervizcsomagja. Ha valaki akkor, illetve azóta sem telepítette az 1. szervizcsomagot, nem kell aggódnia: az 1. szervizcsomagban szereplő valamennyi frissítés és javítás a 2. szervizcsomagban is megtalálható.

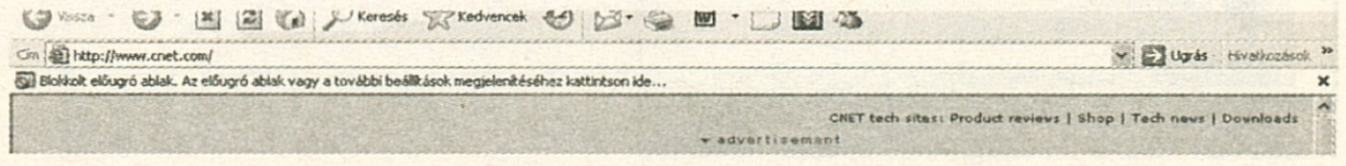
1.4 A Windows XP 2. szervizcsomag tartalma

Ismerkedjünk most meg a 2. szervizcsomag legfontosabb szolgáltatásaival, és tekintsük át, hogy ezek segítségével miként védhetjük még hatékonyabban számítógépünket és személyes adatainkat.

1.4.1 Biztonságosabb kommunikáció és böngészés

A 2. szervizcsomag több új szolgáltatást kínál, amelyekkel biztonságosabban internetezhetünk és levelezhetünk. Ezek a következők:

Előugró ablakok blokkolása az Internet Explorerben. A nem kívánt, előugró reklámablakok számának csökkentésével az SP2 kényelmesebb és élvezetesebb böngészést tesz lehetővé.



Az Internet Explorerban az SP2 blokkolja az előugró ablakok többségét

Letöltések nyomon követése az Internet Explorerben. A 2. szervizcsomag figyelmeztet a potenciálisan veszélyes fájlok letöltése előtt, és segítségével blokkolhatók a veszélyesnek ítélt fájlok.

Az Internet Explorer információs sávja. Ez a szolgáltatás részletesebb adatokkal szolgál a web böngészése során bekövetkező eseményekről, így egyszerűbb nyomon követni a folyamatokat, és megfelelni a biztonsági kihívásoknak.

Az Internet Explorer bővítménykezelője. Egyszerűsíti az Internet Explorer bővítményeinek (a webböngészőt kiegészítő programoknak) a kezelését, így növeli a biztonságot, és csökkenti a rendszerösszeomlások valószínűségét.

Az Outlook Express adatvédelmi frissítése. Segítségével csökkenthető a nem kívánt levelek száma, mert megnehezíti az esetleges levélszemétküldők számára azt, hogy meggyőződjenek e-mail címünk érvényességéről.

Mellékletkezelő. Megfigyeli és hatástalanítja az esetleg veszélyt jelentő mellékleteket, amelyek az Internet Explorer, az Outlook Express és a Windows Messenger használatán keresztül terjedő vírusokat tartalmazhatnak.

1.4.2 Hatékony biztonsági segédeszközök

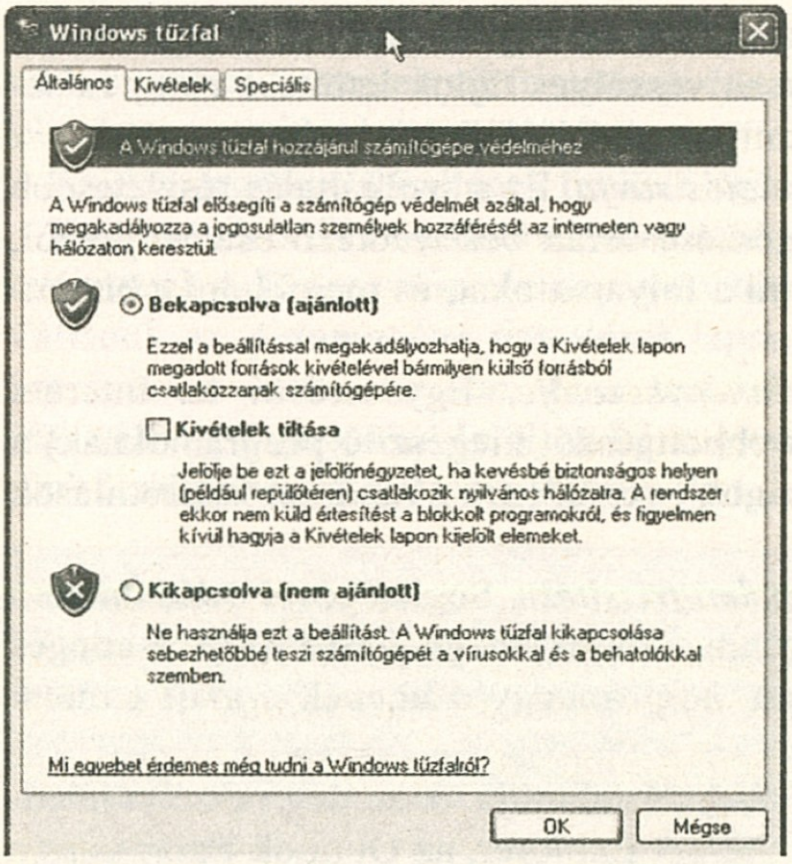
Az új szolgáltatások mellett a 2. szervizcsomag különféle biztonsági segédeszközöket is tartalmaz.

Windows Biztonsági központ. Segítségével egyszerűen nyomon követhető a biztonsági rendszer állapota, és a fontos biztonsági beállítások egy helyen, kényelmes eszközökkel felügyelhetők.

A Windows tűzfal frissítése. Az alapértelmezés szerint automatikusan bekapcsolt továbbfejlesztett tűzfal segít a Windows XP felhasználóinak a vírusok, a férgek, valamint az interneten terjedő egyéb veszélyes fenyegetések elleni védelemben.

A Windows tűzfal egyszerű kompatibilitási beállításai. A Windows tűzfal beállításainál megadható, hogy a tűzfal együttműködjön kedvenc internetes alkalmazásainkkal és az otthoni hálózatunkkal.

A Windows tűzfal rendszerindítási és -leállítási funkciói. Kiterjesztik a Windows tűzfal nyújtotta védelmet a rendszer indítására és leállítására



A tűzfal megújult, és alapértelmezésben aktivizálva van

is, így a számítógép már a bekapcsolástól kezdve egészen a kikapcsolásig kiemelt védelemben részesül.

Továbbfejlesztett automatikus frissítések. A Windows XP naprakész frissítései automatikusan rendelkezésére állnak. A telefonos hálózattal rendelkező felhasználók számára új technológiát fejlesztettek ki a frissítések hatékonyabb letöltése érdekében.

1.4.3 Felhasználóbarát újítások

A 2. szervizcsomag több olyan újítást is tartalmaz, amelyek a felhasználók kényelmét szolgálják.

Vezeték nélküli hálózatok továbbfejlesztett támogatása. A vezeték nélküli hálózatok megkeresése és a csatlakozás fejlettebb technológiával, de ugyanakkor lényegesen egyszerűbben történik.

Bluetooth technológiák. A számítógép egyszerűbben csatlakoztatható a legújabb Bluetooth-eszközökhöz, például billentyűzetekhez, mobiltelefonokhoz és PDA eszközökhöz.

A Windows Media Player 9-es verziója. Fokozott biztonsági beállítások mellett kínál lehetőséget a zenehallgatásra, illetve filmek és szélessávú médiatartalom lejátszására.

DirectX frissítés. A Microsoft DirectX technológiája a legfejlettebb játék- és grafikai funkciókat bocsátja a felhasználók rendelkezésére.

2 Technológiai áttekintés

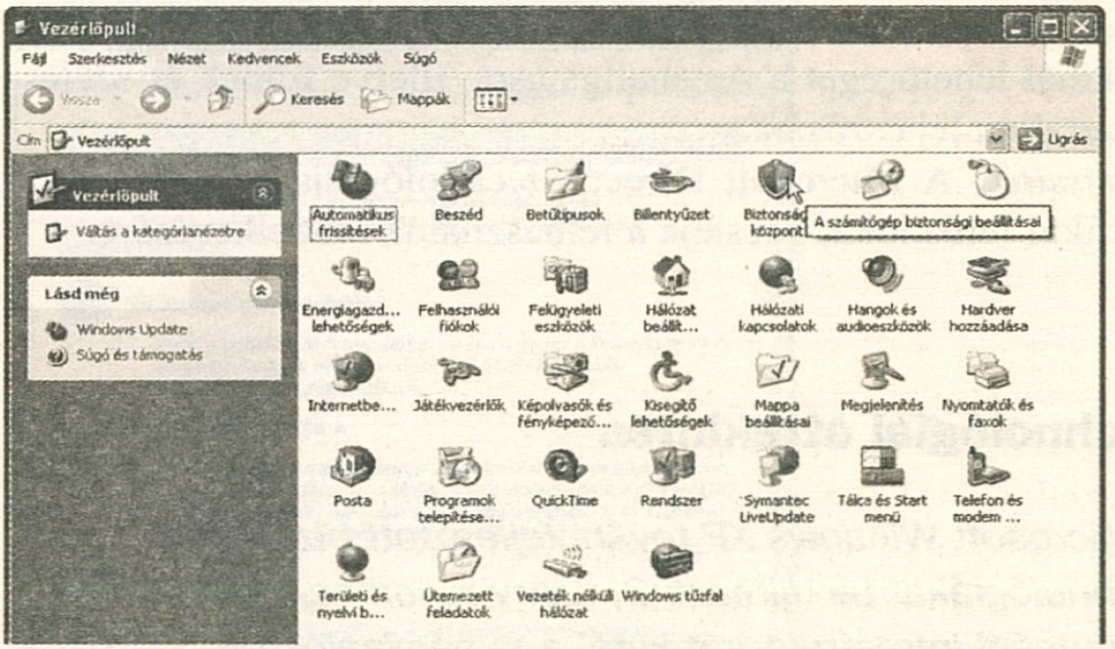
A Microsoft Windows XP továbbfejlesztett biztonsági technológiákat tartalmazó 2. szervizcsomagja bővített biztonsági infrastruktúrát kínál a felhasználóknak a vírusok, férgek és behatolók elleni hatékony védelemhez. A szervizcsomag emellett jobb kezelhetőséget és felügyelhetőséget is biztosít, valamint kellemesebb és következetesebb felhasználói élményt nyújt. Ez a fejezet a Windows XP 2. szervizcsomagjában megjelent legfontosabb változásokat és fejlesztéseket mutatja be.

2.1 Windows Biztonsági központ

A *Windows Biztonsági központtal* egy helyen tekinthetjük meg a biztonsági állapotra vonatkozó adatokat, módosíthatjuk a biztonsági beállításokat, valamint elérhetjük a biztonsági problémákkal kapcsolatos tudnivalókat.

A Biztonsági központ a *Vezérlőpulton* belül található, és a *Windows tűzfal,* az *Automatikus frissítések* szolgáltatás és *vírusvédelmi szoftver* biztonsági összetevők állapotát jelzi.

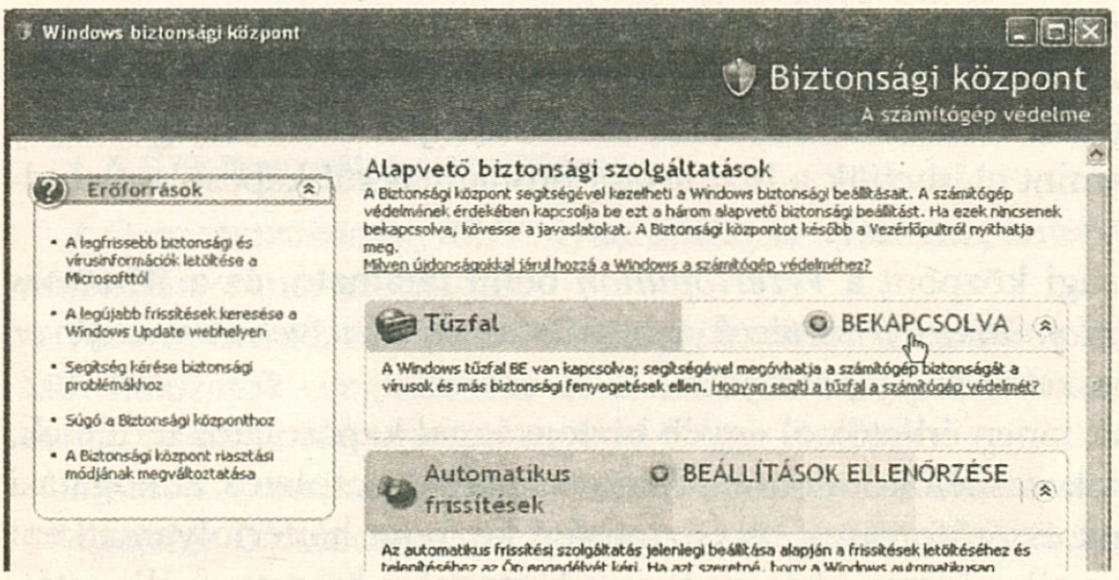
Ugyancsak innen érhetők el egyéb biztonsággal kapcsolatos területek, illetve innen kereshetők különféle biztonsággal kapcsolatos támogatási szolgáltatások és erőforrások. A Biztonsági központ háttérfolyamatként fut, állandóan ellenőrizve e három fontos biztonsági összetevő állapotát.



A Biztonsági központ a rendszertálcáról vagy a Vezérlőpultról is elérhető

2.1.1 Windows tűzfal

Tűzfalat általában minden esetben ajánlatos használni, az internetkapcsolat típusától (telefonos, kábeles modem vagy DSL) függetlenül. Ha a tűzfal nem aktiválódik, amikor az internethez kapcsolódunk, előfordulhat, hogy hackerek megpróbálnak jogosulatlanul hozzáférni számítógépünkhöz, és arra olyan kártékony kódot telepíteni, amely megsemmisítheti a fájlokat, vagy a rendszer hibás működéséhez vezethet.



A Biztonsági központ jelzi a tűzfal állapotát

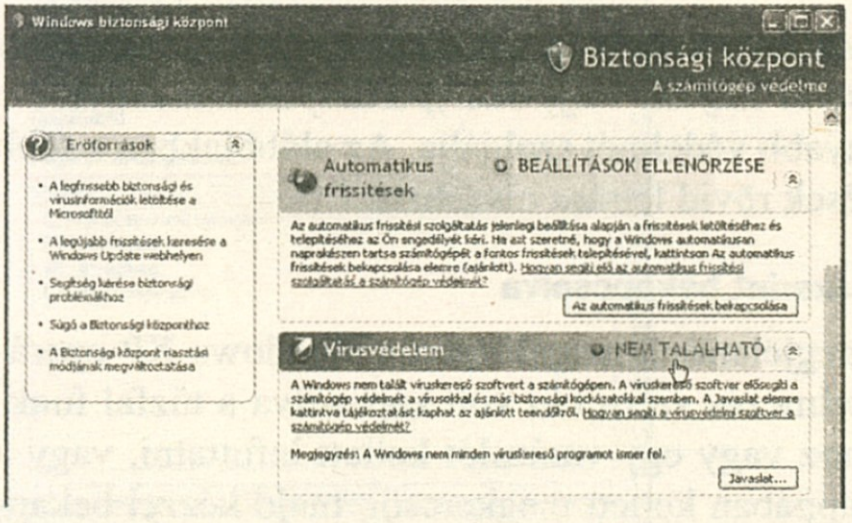
A *Windows tűzfal* a 2. szervizcsomaggal együtt kerül forgalomba, és alapértelmezés szerint már rendszerindításkor működésbe lép. A Biztonsági központ folyamatosan ellenőrzi, hogy a Windows tűzfal be van-e kapcsolva, és figyelmeztet arra, ha nem működik.

2.1.2 Automatikus frissítések

A Windows Biztonsági központ azt is folyamatosan figyeli, hogy az *Automatikus frissítések* funkció a javasolt beállítást használja-e: „A számítógéphez ajánlott frissítések automatikus letöltése és telepítése: <minden nap a következő időpontban: 3:00>". Ha az Automatikus frissítések funkció ki van kapcsolva, vagy az ajánlottól eltérő beállításokat használ, a Windows Biztonsági központ figyelmeztetést küld.

2.1.3 Vírusvédelem

A Windows Biztonsági központ ellenőrzi a vírusvédelmi szoftver jelenlétét, továbbá azt, hogy a szoftver mennyire naprakész, és hogy be van-e kapcsolva a valósidejű ellenőrzés. Ezáltal egyszerűbben megvédhetjük számítógépünket az adatokra és az értékes erőforrásokra nézve veszélyes vírusoktól és férgektől.



A Biztonsági központ ellenőrzi az antivírus szoftver jelenlétét

Amennyiben e biztonsági összetevők valamelyike hiányzik, vagy olyan beállítást használ, amely gyengíti a számítógép biztonságát, a Windows Biztonsági központ vörös pajzs ikon formájában látható az ér-

tesítési területen, és a felhasználó bejelentkezésekor figyelmeztetést is megjelenít. Az ikonra vagy a figyelmeztetésre kattintva megnyílik a Windows Biztonsági központ. Itt megtalálhatjuk a probléma leírását és az elhárítására vonatkozó javaslatot.

Ha a Windows Biztonsági központ által nem érzékelt tűzfalat vagy vírusvédelmi szoftvert használunk, a beállítások módosításával elkerülhető, hogy a kérdéses összetevővel kapcsolatos értesítéseket kapjunk.

A Windows Biztonsági központtal egyszerűen ellenőrizhető, hogy a tűzfal aktív-e, a vírusvédelmi szoftver naprakész-e, illetve hogy a számítógép folyamatosan frissítve van-e a Microsoft által közzétett legújabb kiemelt fontosságú frissítésekkel.

Info

A Windows Biztonsági központról, valamint a Windows XP 2. szervizcsomagjában megjelent egyéb változásokról és fejlesztésekről a www.microsoft.com/hun/windowsxp/sp2 webhelyen olvasható további részletes információ.

2.2 Windows tűzfal

A 2. szervizcsomag számos jelentős újítást kínál a *Windows tűzfalhoz* (korábban *Internetkapcsolat tűzfala* vagy *ICF*), amelyek mindegyike a számítógép még hatékonyabb védelmét szolgálja. Az alábbiakban a főbb változtatások és fejlesztések rövid leírása olvasható.

2.2.1 Alapértelmezés szerint bekapcsolva

A 2. szervizcsomag megjelenését megelőzően a Windows XP operációs rendszerben alapértelmezés szerint ki volt kapcsolva a tűzfal funkció. A tűzfal aktiválásához vagy egy varázslót kellett lefuttatni, vagy a *Hálózati kapcsolatok* mappában kellett megkeresni, majd kézzel bekapcsolni azt.

A 2. szervizcsomag telepítése után a Windows tűzfal alapértelmezés szerint be van kapcsolva, így hatékonyabb alapértelmezett védettséget kínál minden új telepítés és frissítés esetén. Ez a funkció a rendszerhez hozzárendelt új hálózati kapcsolatok védelmét is szolgálja.

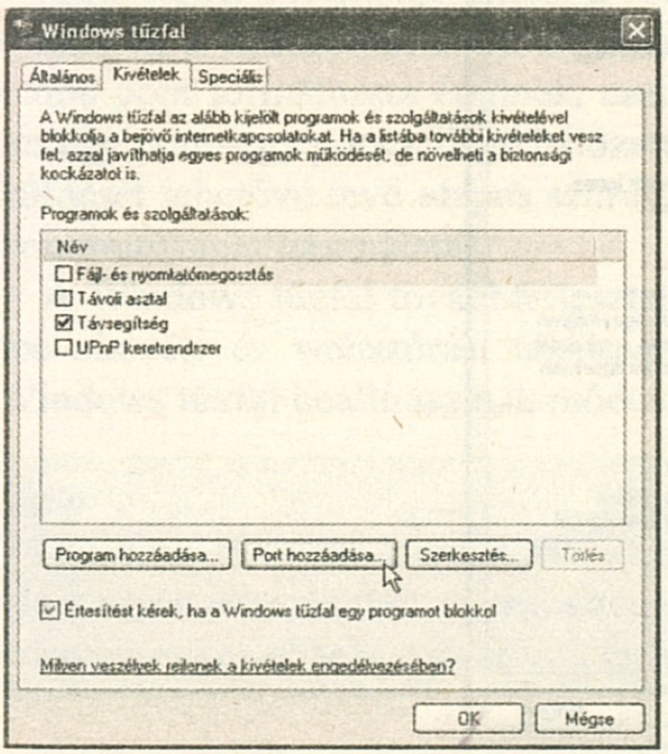
2.2.2 Védelem a rendszer indításakor

A Windows operációs rendszer korábbi verzióiban a hálózat indítása és a tűzfal aktiválódása közben a számítógép egy rövid időn keresztül ki volt téve a nem kívánt támadásoknak.

A 2. szervizcsomag telepítését követően a tűzfal a rendszer indításakor és leállításakor úgynevezett rendszerindítási szűrőt alkalmaz, ezáltal kizárja, hogy ez idő alatt a rendszer védtelenné váljon. A Windows tűzfal betöltését és elindulását követően a rendszer betölti a tűzfal beállításait, és eltávolítja az indítás során alkalmazott szűrőket. A számítógép így sokkal védettebbé válik a rendszer indítása és leállítása idején.

2.2.3 A Windows tűzfal kivétellistája

Hálózati vagy internetkapcsolatot és kétirányú kommunikációt igénylő program futtatásakor biztonsági figyelmeztetés jelenhet meg. Számos többrésztvevős internetes játék például olyan portokat használ, amelyek a Windows tűzfalban alapértelmezés szerint le vannak tiltva. Ezek gyakran ugyanazok a portok, amelyeken keresztül a hackerek és a férgek megpróbálnak betörni a számítógépre.



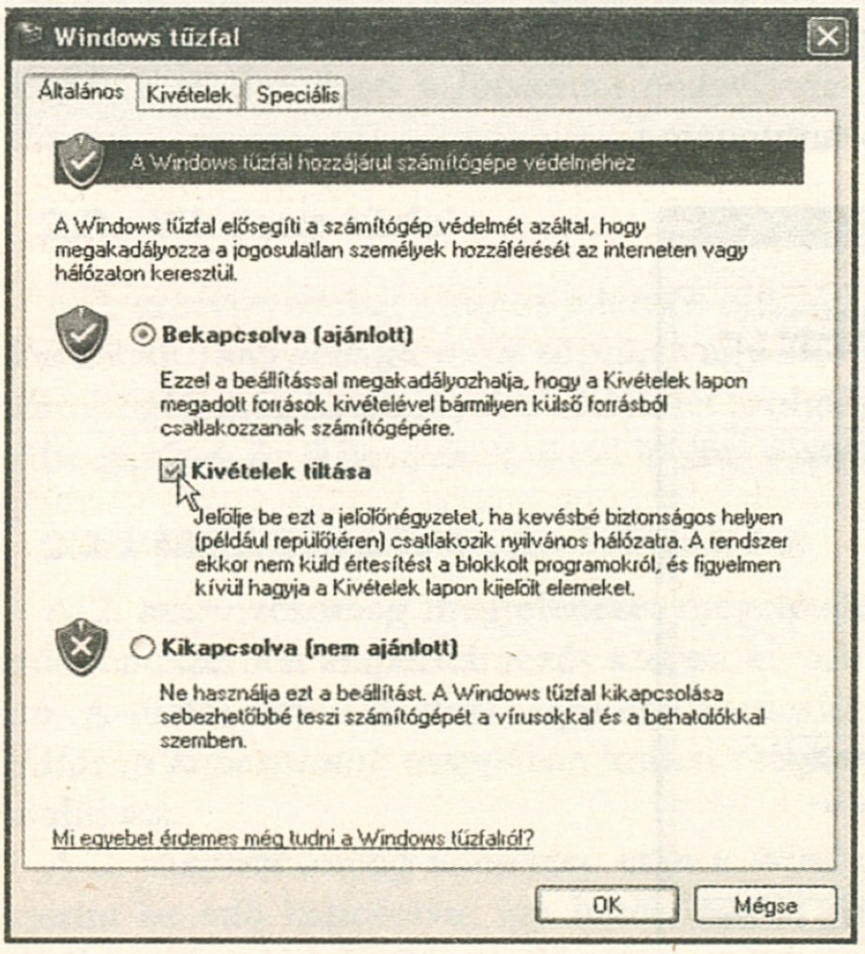
A Kivételek fül alatt megnyithatunk egy portot is kedvenc játékaink számára (a szükséges port számához tanulmányozzuk a játék kézikönyvét)

Játékhoz szükséges port megnyitásához vegye fel a kívánt portot a Windows tűzfal kivételeket tartalmazó listájára. A port csak játék közben nyílik meg, és azonnal bezárul, amikor a felhasználó kilép a játékból.

Azáltal, hogy a rendszer ezeket a portokat kizárólag játék vagy egyéb program futtatása közben nyitja meg, a számítógép sokkal védettebbé válik a rosszindulatú támadásokkal szemben.

2.2.4 A Nem engedélyez kivételt üzemmód

Ezzel a funkcióval egyszerre kapcsolhatjuk ki a Windows tűzfal kivétellistáján szereplő valamennyi kivételt. Bár ezekre a kivételekre bizonyos programok futtatásához szükség van, sok esetben a nagyobb biztonság érdekében érdemesebb kikapcsolni őket. Ha például internetkávézóban vagy reptéren használjuk a számítógépünket, vírusoknak és egyéb biztonsági szempontból káros tényezőknek tesszük ki azt.



A Kivételek tiltása jelölőnégyzet kipipálása maga után vonja, hogy akkor se kell aggódnunk, ha nyilvános helyen használjuk a számítógépünket

A Windows tűzfal *Nem engedélyez kivételt* beállításának kiválasztásával akkor sem kell aggódnunk, ha nyilvános helyen használjuk a számítógépünket. Amikor a számítógépet biztonságosabb környezetben üzemeltetjük, újra bekapcsolhatjuk a kivételek listáját.

2.2.5 Alapértelmezések visszaállítása

Idővel, például programoknak vagy portoknak a Windows tűzfal kivétellistájára való felvételével véletlenül olyan konfiguráció is előfordulhat, amely engedélyezi a Windows tűzfalon keresztül a kéretlen bejövő forgalmat, így veszélyezteti a számítógép biztonságát. A Windows tűzfal korábbi verzióiban nem lehetett kényelmesen visszaállítani az eredeti beállításokat.

Ezzel a lehetőséggel az alapértelmezett beállításokra állíthatjuk vissza a Windows tűzfalat. További előnyt jelent, hogy az alapértelmezett értékek módosításával egyéni konfigurációk hozhatók létre.

2.2.6 Csoportos címzés és webszórás

A csoportos címzés és a szórásos hálózati forgalom körébe tartozik többek között a *telekonferencia,* a *videokonferencia,* az *adatfolyam-közvetítés* és a *webszórás.* Ezek a kommunikációs formák mind egy pont –több pont formátumra épülnek, ezért a tűzfalaknál általában használatos egy pont–egy pont jellegű hálózati kommunikációt, például az e-mail küldését lehetővé tevő alapos szűrés megakadályozhatja a webszórásos kommunikáció használatát.

A Windows tűzfal továbbfejlesztett támogatást kínál, hogy a csoportos címzést és webszórást alkalmazó programok és szolgáltatások a Windows tűzfal beállításainak módosítása nélkül is működjenek.

Info

A Windows tűzfalról, valamint a Windows XP 2. szervizcsomagjában megjelent egyéb változásokról és fejlesztésekről a www.microsoft.com/hun/windowsxp/sp2 webhelyen olvasható további részletes információ.

2.3 Internet Explorer

Az alábbiakból kiderül, hogy a 2. szervizcsomagban található technológiák hogyan teszik biztonságosabbá a webböngészést, miközben a böngészés még felügyelhetőbbé válik.

2.3.1 Előugró ablakok blokkolása az Internet Explorerben

Az *Előugró ablakok blokkolása az Internet Explorerben* új funkció a 2. szervizcsomagban, amellyel megelőzhető, hogy megjelenjenek a nem kívánt előugró reklámablakok. Az *Internet Explorer* böngésző *Eszközök* menüjéből elérhető funkcióval hatékonyabban felügyelhető a böngészés, ugyanakkor a felhasználó döntheti el, hogy mely webhelyek előugró ablakait blokkolja, és mely webhelyekét nem.

A funkció alapértelmezés szerint be van kapcsolva, de az Internet Explorer előugró ablakokat blokkoló szolgáltatása bizonyos esetekben mégis engedélyezi az előugró ablakok megjelenését. Ilyen eset például, ha az előugró ablakot generáló webhelyet felvették az *Engedélyezett webhelyek* listára, ha az előugró ablakot generáló webhely a *Megbízható helyek* vagy a *Helyi intranet* zónában szerepel, vagy ha a webhelyről indított *ActiveX*-vezérlők nyitják meg az előugró ablakot.

Ha egy webhely előugró ablakot nyit meg, miközben be van kapcsolva az előugró ablakok blokkolása az Internet Explorerben, és az Internet Explorer blokkolja az ablak megjelenését, akkor a felhasználó üzenetet kap az Internet Explorer információs sávján, valamint hangjelzés is hallható.

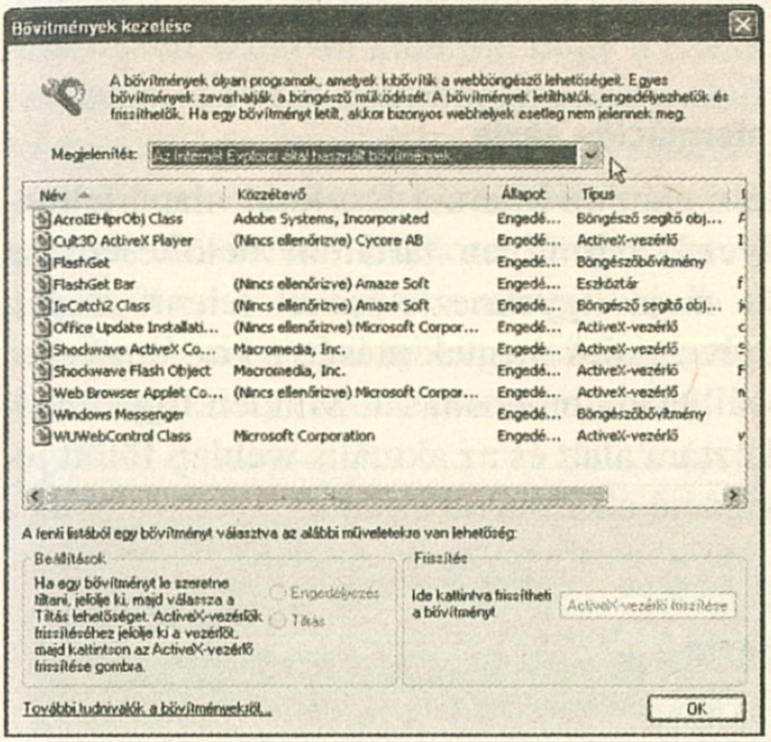
Az értesítésre kattintva több lehetőség közül választhatunk, mégpedig az előugró ablakok ideiglenes engedélyezése, a webhely előugró ablakainak mindenkori engedélyezése és a beállítások közül.

Az engedélyezett webhelyek listájára további webhelyek is felvehetők, illetve eltávolíthatók a listán szereplő webhelyek, be- vagy kikapcsolhatók az értesítő hangjelzések stb.

2.3.2 Az Internet Explorer bővítménykezelője

Bár az Internet Explorer bővítményei, például az ActiveX-vezérlők, a böngésző súgóobjektumai és az eszköztárak hatékonyabbá tehetik a böngészést, bizonyos esetekben stabilitási problémákat okozhatnak. Ezenkí-

vül biztonsági szempontból is kockázatosak, mert előfordulhat, hogy veszélyes kódot tartalmaznak. Korábban, amikor a felhasználók körében még gyakori volt a rendszer összeomlása, nem lehetett egyszerűen diagnosztizálni, hogy a problémát valamelyik bővítmény okozta-e.



Az újdonsült bővítménykezelővel végre egyszerűen hozzáférhetők az Explorer bővítményei

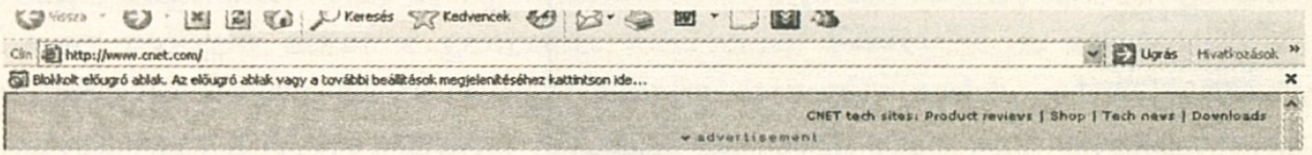
A rendszer nagyobb biztonsága és stabilitása érdekében az Internet Explorer *Eszközök* menüjéből megnyitható *Bővítménykezelővel* megtekinthető és felügyelhető az Internet Explorer által betölthető bővítmények listája. Itt említhető például, hogy egy akaratlanul telepített bővítmény titokban rögzítheti a felhasználónak a különböző webhelyeken végzett összes tevékenységét, és jelentheti azt egy központi kiszolgálónak. Korábban az efféle problémát okozó bővítmények azonosításához és eltávolításához speciális szoftverre és technikai hozzáértésre volt szükség.

Az Internet Explorer *Bővítménykezelőjével* a bővítmények azonosítása és kikapcsolása sokkal egyszerűbbé vált. A bővítmények egyesével is be- vagy kikapcsolhatók, továbbá a bővítmény használatának gyakoriságára vonatkozó információ és a bővítmény kiadójának neve is megtekinthető.

Az ActiveX-vezérlők egyesével is frissíthetők. A vezérlő frissítése esetén egy webes keresés indul el a vezérlő eredeti helyén, hogy megkeresse a rendelkezésre álló frissítést. Amikor megtalálta, a rendszer letölti és telepíti a frissítést. Az ActiveX-vezérlők naprakész verziójának használatával hatékonyabban megelőzhetők a rendszerhibák és a biztonsági problémák.

2.3.3 Az Internet Explorer információs sávja

A 2. szervizcsomag telepítése után az Internet Explorer alapértelmezett beállításai nem engedélyezik bármilyen tartalom betöltését. Az Internet Explorer információs sávja figyelmeztetéseket jelenít meg a blokkolt tartalomról, lehetővé téve annak megtekintését, a korlátozás kezelését, valamint az érintett beállítások módosítását. Minden figyelmeztetés az Internet Explorer eszköztára alatt és az aktuális weblap fölött jelenik meg, és a következő navigáció alkalmával eltűnik.



Az információs sáv figyelmeztetést jelenít meg a blokkolt tartalomról

A figyelmeztetésként küldött információ így mindig jól látható, és a rendelkezésre álló lehetőségek is könnyen elérhetők. Az információs sávon megjelenő szöveg a figyelmeztetéstől függően változik. A gyakori üzenetek közé tartozik például *„A webhelyhez szükség lehet a következő ActiveX-vezérlőre:"* üzenet. Az Internet Explorer információs sávjára kattintva megnyílik a figyelmeztetéshez kapcsolódó menü, amelyről választhatunk, hogy melyik tartalmat tekintjük meg, és melyiket blokkoljuk.

2.3.4 Helyi számítógép zóna zárolása

Amikor az Internet Explorer weblapot nyit meg, a lap helye és a hozzárendelt biztonsági zóna alapján korlátozza az adott lap által elvégezhető műveleteket. Többféle biztonsági zóna létezik, és mindegyikhez más és más megszorítások tartoznak. Az interneten található lapok általában a szigorúbban korlátozott *Internet* biztonsági zónába tartoznak. A válla-

lati hálózaton található lapok általában a *Helyi intranet* biztonsági zónához tartoznak, és kevesebb megszorítás vonatkozik rájuk.

A 2. szervizcsomag megjelenése előtt feltételezték, hogy a helyi fájlrendszeren található tartalom biztonságos, ezért a *Helyi számítógép* biztonsági zónát rendelték hozzá, amely kevés megszorítást tartalmazott. Időközben azonban kiderült, hogy a hackerek gyakran megpróbálják kihasználni a Helyi számítógép zóna csekély korlátozásaiból adódó lehetőségeket, így az veszélyes lehet a számítógépre vagy a rendszerre.

A 2. szervizcsomag alapértelmezett beállításai több korlátozást alkalmaznak az Internet Explorer Helyi számítógép zónájára. Tiltott tartalom elindulása esetén figyelmeztetés jelenik meg az Internet Explorer információs sávján, így a felhasználó döntheti el, hogy rákattintva eltávolítja-e a korlátozást, és futtatja-e a tartalmat.

Info

Az Internet Explorer böngészőről, valamint a Windows XP 2. szervizcsomagjában megjelent egyéb változásokról és fejlesztésekről a www.microsoft.com/hun/windowsxp/sp2 webhelyen olvasható további részletes információ.

2.4 Outlook Express

A 2. szervizcsomagnak az *Outlook Express* programra vonatkozó módosításai és továbbfejlesztései még több lehetőséget kínálnak az adatvédelem és a biztonság területén, többek között nagyobb biztonságot nyújtanak az e-mail üzenetekben továbbított, esetleges veszélyt jelentő programokkal szemben.

2.4.1 Egyszerű szöveges üzemmód

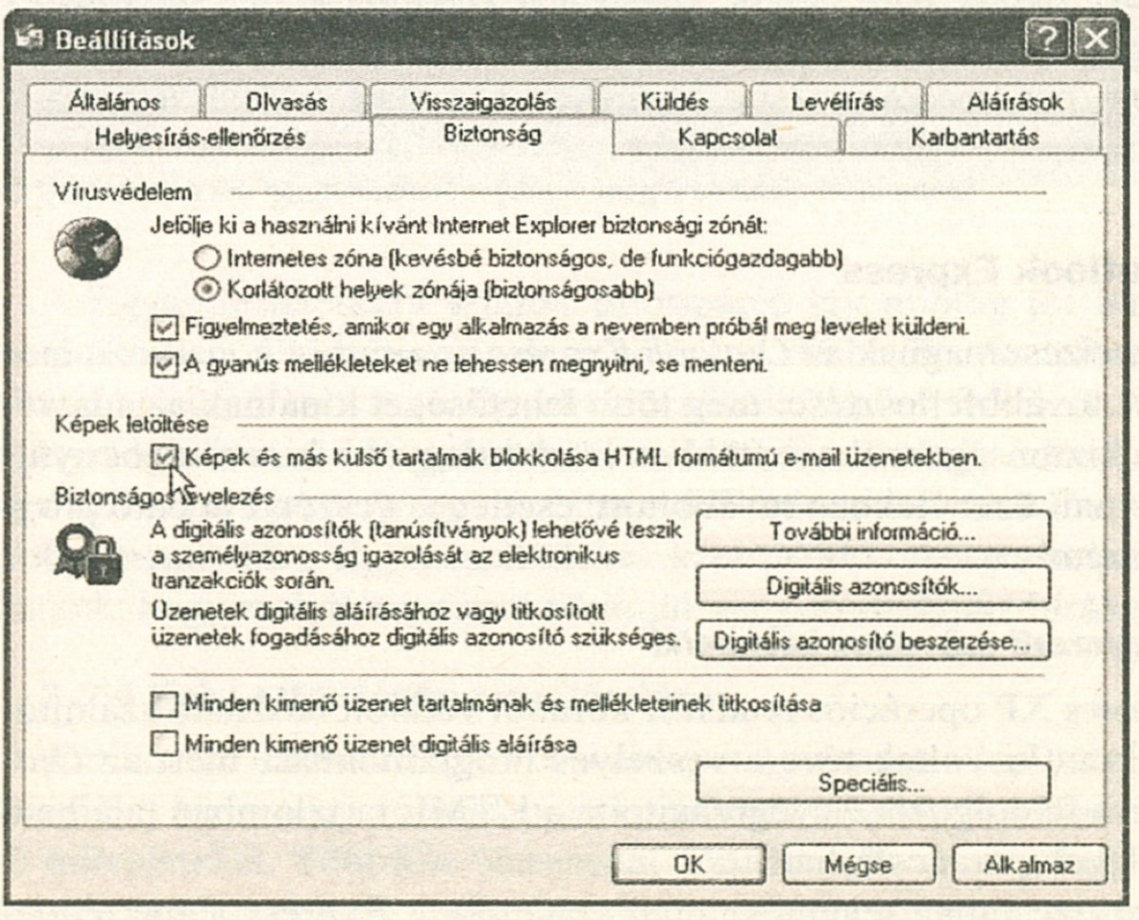
A Windows XP operációs rendszer korábbi verzióit használó számítógépek gyakran ki voltak téve a veszélyes programoknak, mert az *Outlook Express* feldolgozta és végrehajtotta a HTML tartalomban található HTML fejlécek parancsfájljait.

A 2. szervizcsomag telepítése után az Outlook Express alapértelmezett nézete az *Egyszerű szöveges mód* lesz, amely további akadályt jelent

a fejléc parancsfájljaiban elrejtett veszélyes programoknak. Minthogy az egyszerű szöveges e-mail üzenetek használata esetén nem szükséges a HTML-fejléc feldolgozása, ez a változtatás általában nem is vehető észre. Az Outlook Express Nézet menüjében továbbra is rendelkezésre áll az üzenetek HTML nézetben való megtekintésének a lehetősége.

2.4.2 HTML tartalom blokkolása

Ezzel az alapértelmezés szerint bekapcsolt funkcióval kiszűrhetők az Outlook Express programból az ismétlődő szemétlevelek, mert a funkció megelőzi, hogy a felhasználó önszántán kívül megerősítse e-mail címének valódiságát a kéretlen levelek feladói számára. A levélszemét-üzenetekben gyakran távoli webkiszolgálókon található képekre mutató hivatkozások vannak elrejtve. Ezek a képek többnyire nagyon kicsik, gyakran csak egyetlen képpont méretűek, így a címzett nem is veszi észre azokat az üzenetben.



A külső HTML tartalom letöltésének tiltása funkció a Eszközök/Beállítások/Biztonság lapon kapcsolható ki/be

Ilyen képet tartalmazó e-mail üzenet megnyitásakor az Outlook Express korábbi verziói automatikusan kapcsolatba léptek a webkiszolgálóval, hogy letöltsék és megjelenítsék a képeket. A válaszoló kiszolgáló a kérésre megerősítette a felhasználó e-mail címét, majd fel is vehette azt egy megerősített e-mail címeket tartalmazó listára, amelynek alapján a későbbiekben további levélszemetet küldhetett a felhasználónak.

A *külső HTML tartalom letöltésének letiltásával* az Outlook Express alapértelmezett működése annyiban módosul, hogy csak akkor lép kapcsolatba a webkiszolgálóval külső tartalom letöltése céljából, ha a felhasználó jóváhagyja azt. A felhasználó választhat, hogy letölti-e a tartalmat, vagy sem, illetve ki is kapcsolhatja ezt a funkciót. A funkció működése az Outlook Express *Eszközök* menüjéből megnyitható *Beállítások* párbeszédpanel *Biztonság* lapján állítható be.

A funkció a telefonos kapcsolatot alkalmazó felhasználók által tapasztalt egyik problémára is megoldást nyújt. Korábban, ha az e-mail üzenetek letöltése után a felhasználó megszakította a kapcsolatot, az üzenetek kapcsolat nélküli megtekintése során a modem automatikusan tárcsázni kezdett a külső tartalom letöltéséhez. Mivel azonban az e-mail üzenetekben található szinte valamennyi külső HTML hivatkozás az Internet zónában levő helyekre mutat, alapértelmezés szerint nem jelenik meg a tartalom, így telefonos hálózati kapcsolatra sincs szükség.

2.4.3 A mellékletkezelő integrációja

Az Outlook Express támogatja a 2. szervizcsomagban található *mellékletkezelő* felületet, amely az e-mail üzenetek mellékleteinek ellenőrzését végzi. A mellékletkezelő következetes használatot és a mellékletek biztonsága szempontjából még egységesebb megközelítést kínál a Windows alkalmazások között.

Info

Az Outlook Express programról, valamint a Windows XP 2. szervizcsomagjában megjelent egyéb változásokról és fejlesztésekről a www.microsoft.-com/hun/windowsxp/sp2 webhelyen olvasható további részletes információ.

3 Telepítés és használat

A Windows XP továbbfejlesztett biztonsági technológiákat tartalmazó 2. szervizcsomagját (SP2) telepítve elősegítjük a számítógép és a személyes adatok védelmét a behatolók, a vírusok és a férgek ellen. Ez a fejezet lépésről-lépésre haladva mutatja be a telepítés menetét, valamint egyszerű útmutatásokat kínál a továbbfejlesztett biztonsági technológiák használatának megkönnyítésére.

3.1 Mire jó a szervizcsomag?

Ha a számítógépünkre a *Windows XP* operációs rendszert telepítettük, a Windows XP 2. szervizcsomagját is telepítenünk kell, amely a kifejezetten a Windows XP rendszerhez kifejlesztett új biztonsági segédeszközök révén segít védeni a számítógépet a vírusok, a behatolók és a férgek ellen.

A Windows XP 2. szervizcsomagjával kevésbé bonyolult és időigényes a biztonsági beállítások felügyelete és a biztonsági frissítések naprakészen tartása. Az *Internet Explorer* javításaival és a *Windows Media Player* frissítéseivel a Windows XP 2. szervizcsomagja a legújabb technológiákat támogatja, így a lehető legteljesebb élményt nyújtja, mégpedig fokozott biztonság mellett.

A Windows XP 2. szervizcsomagja a *Windows XP Home Edition* vagy a *Windows XP Professional* operációs rendszerrel működő számítógépekhez ajánlott. Ha nemrég vásároltuk a számítógépet, vagy a számítógépen bekapcsoltuk az *Automatikus frissítések* szolgáltatást, elképzelhető, hogy a Windows XP 2. szervizcsomagja már telepítve van a számítógépen.

Az alábbi lépések végrehajtásával ellenőrizhetjük, hogy a számítógépünkön már telepítve van-e a Windows XP 2. szervizcsomagja.

Kattintsunk a *Sajátgép* ikonra a munkaasztalon.

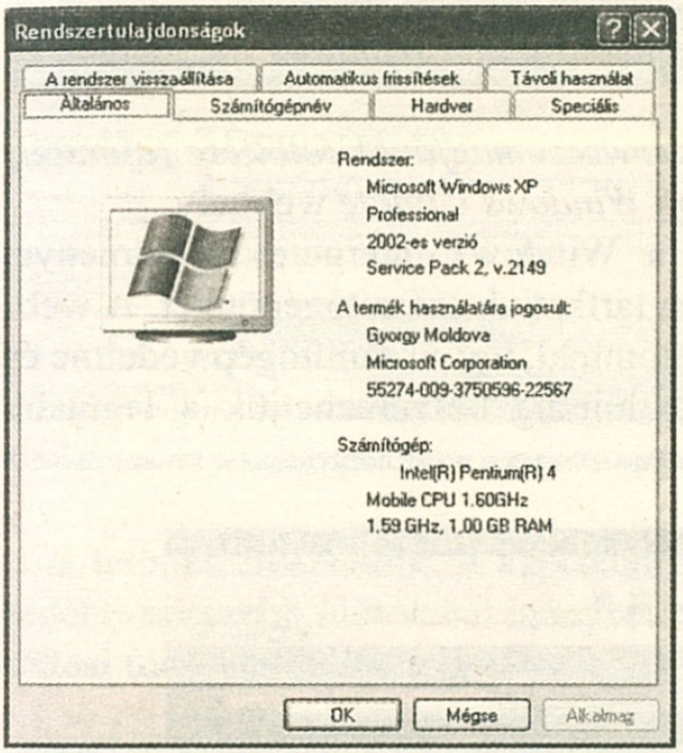
A munkaablakban kattintsunk a *Rendszerműveletek* csoportban levő

Rendszerinformáció megjelenítése parancsra. Megjelenik a *Rendszertulajdonságok* ablak.

Lépjünk az *Általános* panellapra.

Ha a *Rendszer* felirat alatt megjelenített utolsó elem a *Service Pack 2*, akkor már telepítettük a Windows XP 2. szervizcsomagját. Ha a *Szervizcsomag 1* felirat látható, vagy a hely üres, telepíteni kell a Windows XP 2. szervizcsomagját.

Az ablak bezárásához kattintsunk a *Mégse* gombra.



Hogy szükség van-e a szervizcsomag telepítésére, a Rendszertulajdonságok alatt ellenőrizhetjük

3.2 Telepítés előtti ellenőrzőlista

Mielőtt megkezdenénk a 2. szervizcsomag telepítését, a gördülékeny telepítés érdekében haladjunk végig az alábbi ellenőrzőlista lépésein.

Készítsünk biztonsági másolatot a fájlokról.

Célszerű a számítógépen tárolt összes fájlról teljes biztonsági másolatot készíteni. A biztonsági másolatok készítésével kapcsolatos tudnivalókról a Windows XP *Súgó és támogatási* központjában, a *Biztonsági másolatok készítése fájlokról és mappákról* témakörben olvashatunk bővebben.

3.3 Letöltés és telepítés

Miután elvégeztük az ellenőrzőlistában szereplő feladatokat, megkezdhetjük a Microsoft Windows XP továbbfejlesztett biztonsági technológiákat tartalmazó 2. szervizcsomagjának telepítését.

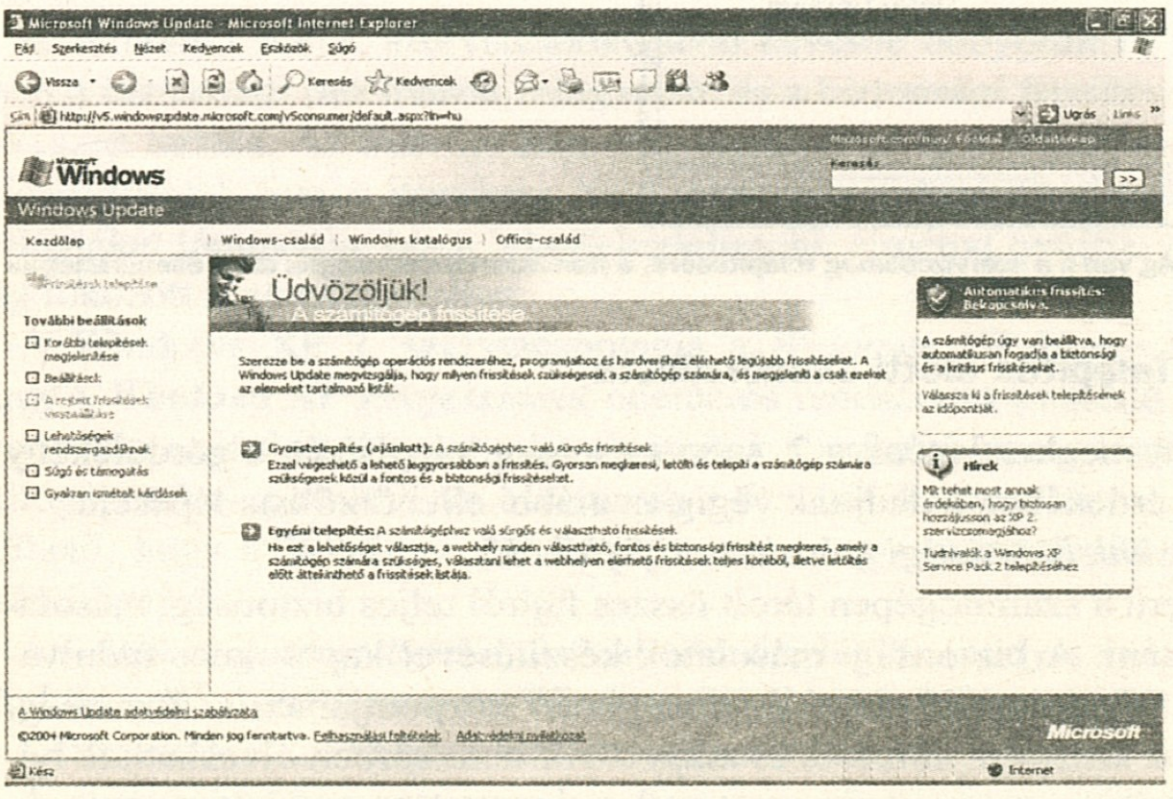
A Windows XP 2. szervizcsomagját a Microsoft webhelyéről tölthetjük le és telepíthetjük.

Az Internet Explorer használatával lépjünk a következő címre: **www.microsoft.com/hun/protect.**

Az *Először:* legördülő menüben jelöljük ki a *Windows XP* elemet, és kattintsunk a *Tovább* gombra.

Kattintsunk a *Windows XP 2. szervizcsomagjának letöltése (ajánlott)* lehetőségre. Megjelenik a *Microsoft Windows Update* webhely.

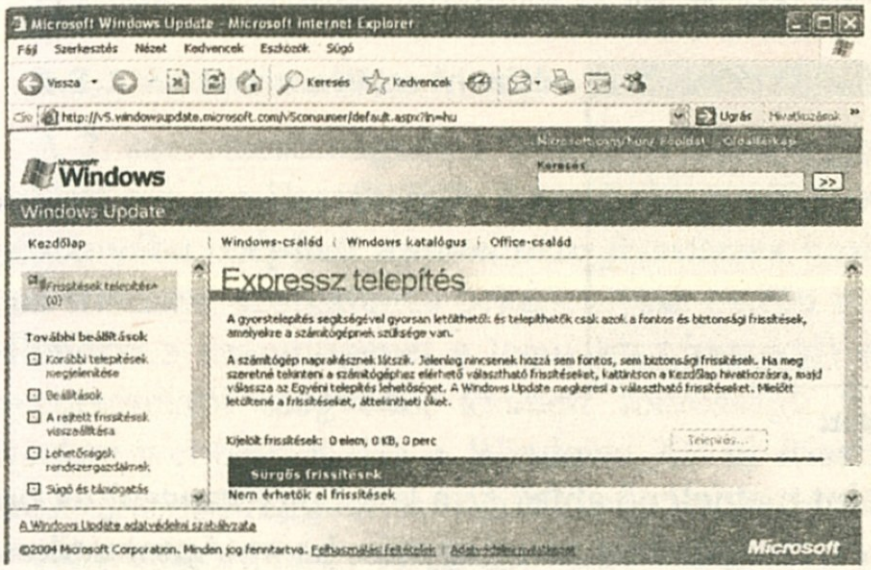
A Windows Update webhely a Windows internetes bővítménye, amelynek segítségével naprakészen tarthatjuk számítógépünket. A webhelyet rendszeresen bővítik új tartalommal, így a számítógép védelme és gördülékeny működése érdekében mindig beszerezhetjük a legújabb frissítéseket és javításokat.



A biztonsági frissítéseket a Windows Update oldaláról tölthetjük le

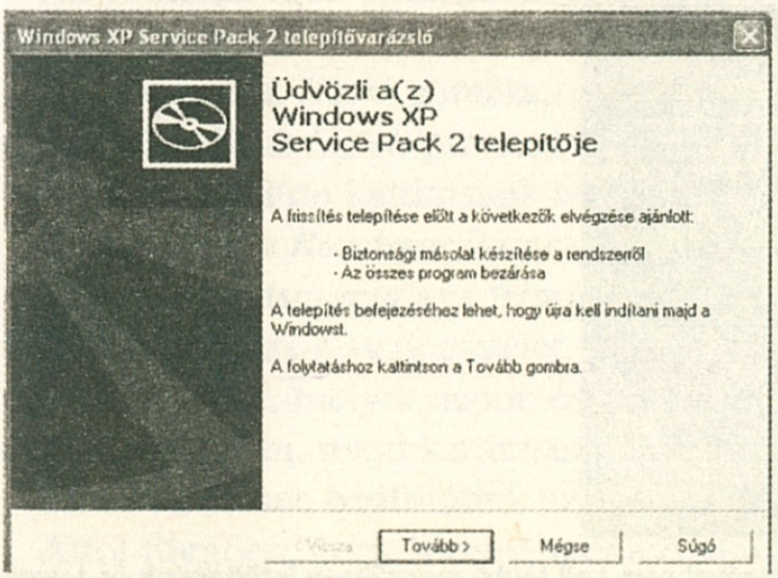
Az *Üdvözöljük!* képernyőn kattintsunk a *Gyorstelepítés (ajánlott)* lehetőségre. Miután a Gyorstelepítés hivatkozásra kattintottunk, a Windows Update ellenőrzi a rendszerünket, hogy meghatározza, milyen frissítésekre van szüksége.

Az *Expressz telepítés* képernyőn kattintsunk a *Telepítés* gombra.



A frissítéseket a legegyszerűbben a gyorstelepítés segítségével tölthetjük le

A letöltés elkezdődik. A kapcsolat sebességétől függően a letöltés rövidebb-hosszabb időt vehet igénybe. Nem kell figyelemmel kísérni a letöltési folyamatot, továbbra is használhatjuk a számítógépet.

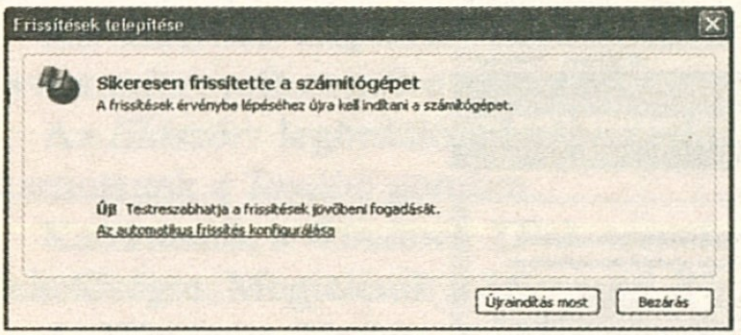


Indul a 2. szervizcsomag telepítővarázslója

A letöltési folyamat befejeztével megjelenik a Windows XP 2. szervizcsomagjának *Végfelhasználói licencszerződése.*

Elindul a 2. szervizcsomag telepítővarázslója. Kattintsunk a *Tovább* gombra.

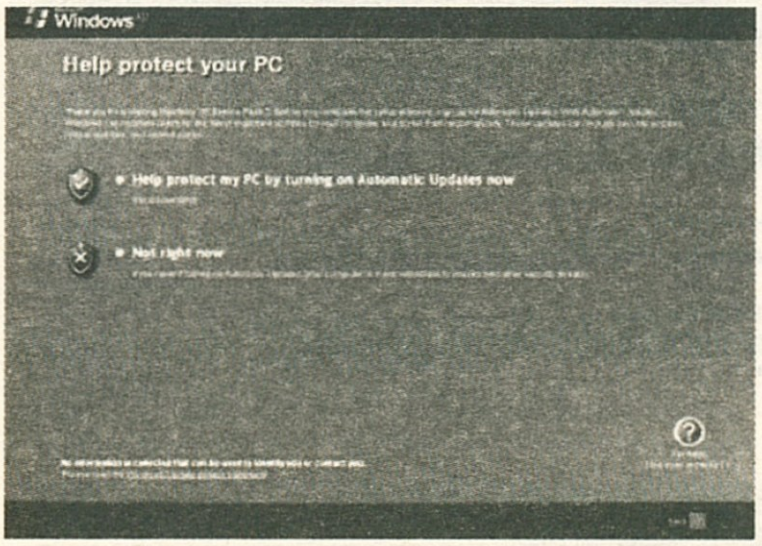
A telepítési folyamat elkészültével kattintsunk az *Újraindítás most* gombra, hogy a telepítést befejezzük.



A telepítés sikeresen befejeződött

A telepítés után elsőként megjelenő ablak arra kér, hogy kapcsoljuk be az *Automatikus frissítések* szolgáltatást (megjegyzés: ha az Automatikus frissítések szolgáltatás beállítása jelenleg *A számítógéphez ajánlott frissítések automatikus letöltése és telepítése,* nem jelenik meg ez a képernyő).

Az Automatikus frissítések bekapcsolása a legegyszerűbb módja a számítógép védelmének a különféle biztonsági fenyegetések ellen. Ekkor nem kell rendszeresen ellenőriznünk a Windows Update webhelyet,



Az Automatikus frissítések bekapcsolásával nem kell többé manuálisan letöltenünk és telepítenünk a frissítéseket

hogy manuálisan letöltsük és telepítsük a legújabb frissítéseket. Az Automatikus frissítések szolgáltatás mindezt helyettünk is elvégzi.

Az Automatikus frissítések bekapcsolásához kattintsunk *A számítógép védelme az automatikus frissítési szolgáltatás azonnali bekapcsolásával (ajánlott)* lehetőségre, majd a *Tovább* gombra.

A 2. szervizcsomag telepítése ezzel befejeződött.

3.3.1 Az Automatikus frissítés használata

A 2. szervizcsomagnak a Windows Update webhelyről való letöltése helyett azt is választhatjuk, hogy bekapcsoljuk a Windows XP minden példányába beépített *Automatikus frissítések* szolgáltatást. Az automatikus frissítési szolgáltatás bekapcsolása esetén a Windows rendszeresen ellenőrzi a számítógépet a legújabb vírusoktól és egyéb biztonsági fenyegetésektől megvédő, kiemelt fontosságú frissítéseket a *Windows Update* webhelyen. Ha a Windows XP új frissítést észlel, a választott beállításoktól függően automatikusan letölti és telepíti a számítógépre.

Nem számít, hogy telefonos vagy szélessávú kapcsolatot használunk, mivel a frissítések letöltése a felhasználók számára észrevétlenül történik, anélkül, hogy zavarná a számítógépen végzett egyéb műveleteket. Ha a frissítések letöltésének befejezte előtt megszakítjuk az internetkapcsolatot, semmi sem vész el. A letöltési folyamat az internethez való következő kapcsolódás alkalmával folytatódik.

Az Automatikus frissítések szolgáltatás bekapcsolása a következőképpen történik.

Kattintsunk a *Start* gombra, vigyük az egeret a *Beállításokra,* majd válasszuk a *Vezérlőpult* parancsot.

A Vezérlőpulton kattintsunk a *Teljesítmény és karbantartás* elemre.

Kattintsunk a *Rendszer* ikonra.

Lépjünk az *Automatikus frissítések* lapra, és jelöljük be *A számítógép automatikus frissítése* négyzetet.

Válasszuk ki, melyik napon és milyen időpontban szeretnénk a frissítéseket telepíteni, majd kattintsunk az *OK* gombra.

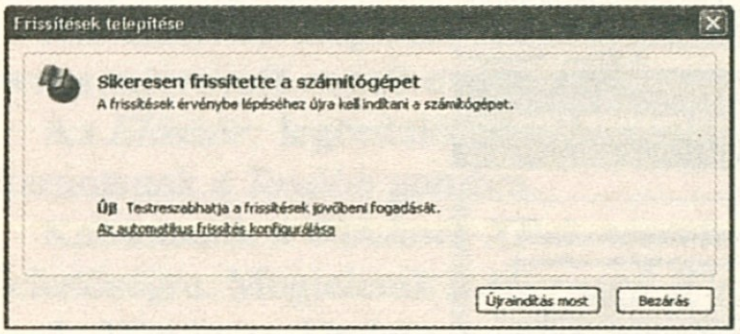
Ezzel sikeresen beállítottuk az Automatikus frissítések szolgáltatást.

Attól függően, hogy hetente mennyi ideig kapcsolódunk az internetre, a Windows XP számára 2–6 hétig is eltarthat a 2. szervizcsomag teljes

A letöltési folyamat befejeztével megjelenik a Windows XP 2. szervizcsomagjának *Végfelhasználói licencszerződése.*

Elindul a 2. szervizcsomag telepítővarázslója. Kattintsunk a *Tovább* gombra.

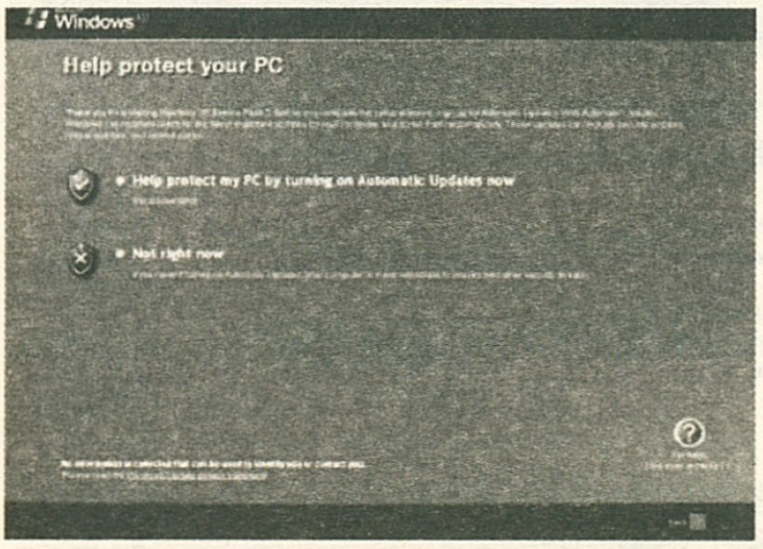
A telepítési folyamat elkészültével kattintsunk az *Újraindítás most* gombra, hogy a telepítést befejezzük.



A telepítés sikeresen befejeződött

A telepítés után elsőként megjelenő ablak arra kér, hogy kapcsoljuk be az *Automatikus frissítések* szolgáltatást (megjegyzés: ha az Automatikus frissítések szolgáltatás beállítása jelenleg *A számítógéphez ajánlott frissítések automatikus letöltése és telepítése,* nem jelenik meg ez a képernyő).

Az Automatikus frissítések bekapcsolása a legegyszerűbb módja a számítógép védelmének a különféle biztonsági fenyegetések ellen. Ekkor nem kell rendszeresen ellenőriznünk a Windows Update webhelyet,



Az Automatikus frissítések bekapcsolásával nem kell többé manuálisan letöltenünk és telepítenünk a frissítéseket

hogy manuálisan letöltsük és telepítsük a legújabb frissítéseket. Az Automatikus frissítések szolgáltatás mindezt helyettünk is elvégzi.

Az Automatikus frissítések bekapcsolásához kattintsunk *A számítógép védelme az automatikus frissítési szolgáltatás azonnali bekapcsolásával (ajánlott)* lehetőségre, majd a *Tovább* gombra.

A 2. szervizcsomag telepítése ezzel befejeződött.

3.3.1 Az Automatikus frissítés használata

A 2. szervizcsomagnak a Windows Update webhelyről való letöltése helyett azt is választhatjuk, hogy bekapcsoljuk a Windows XP minden példányába beépített *Automatikus frissítések* szolgáltatást. Az automatikus frissítési szolgáltatás bekapcsolása esetén a Windows rendszeresen ellenőrzi a számítógépet a legújabb vírusoktól és egyéb biztonsági fenyegetésektől megvédő, kiemelt fontosságú frissítéseket a *Windows Update* webhelyen. Ha a Windows XP új frissítést észlel, a választott beállításoktól függően automatikusan letölti és telepíti a számítógépre.

Nem számít, hogy telefonos vagy szélessávú kapcsolatot használunk, mivel a frissítések letöltése a felhasználók számára észrevétlenül történik, anélkül, hogy zavarná a számítógépen végzett egyéb műveleteket. Ha a frissítések letöltésének befejezte előtt megszakítjuk az internetkapcsolatot, semmi sem vész el. A letöltési folyamat az internethez való következő kapcsolódás alkalmával folytatódik.

Az Automatikus frissítések szolgáltatás bekapcsolása a következőképpen történik.

Kattintsunk a *Start* gombra, vigyük az egeret a *Beállításokra,* majd válasszuk a *Vezérlőpult* parancsot.

A Vezérlőpulton kattintsunk a *Teljesítmény és karbantartás* elemre.

Kattintsunk a *Rendszer* ikonra.

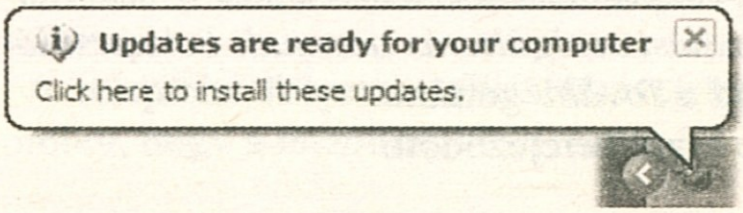
Lépjünk az *Automatikus frissítések* lapra, és jelöljük be *A számítógép automatikus frissítése* négyzetet.

Válasszuk ki, melyik napon és milyen időpontban szeretnénk a frissítéseket telepíteni, majd kattintsunk az *OK* gombra.

Ezzel sikeresen beállítottuk az Automatikus frissítések szolgáltatást.

Attól függően, hogy hetente mennyi ideig kapcsolódunk az internetre, a Windows XP számára 2–6 hétig is eltarthat a 2. szervizcsomag teljes

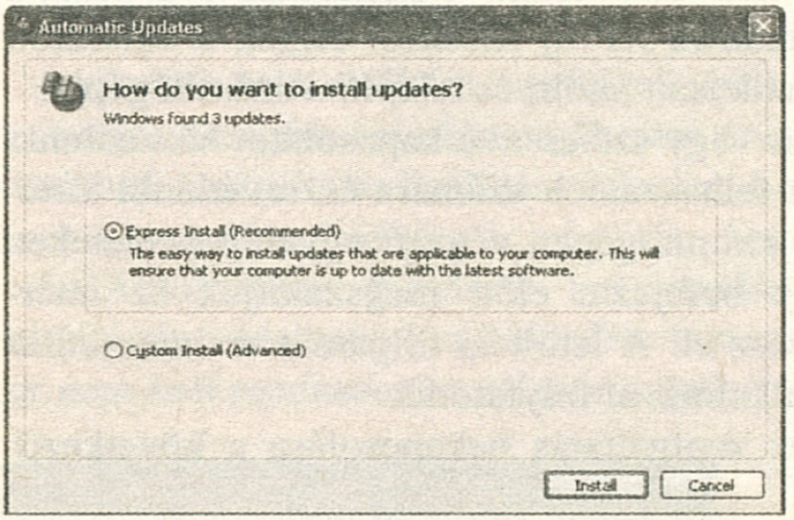
letöltése. A letöltés befejeztével a következő üzenet jelenik meg a képernyő jobb alsó sarkában:



A frissítés sikeres letöltését üzenet jelzi

Az üzenet megjelenése után a 2. szervizcsomag telepítésének befejezéséhez kövessük az alábbi lépéseket.

Ha *A számítógéphez tartozó frissítések készen állnak* üzenetre kattintunk, egy újabb üzenet arra kér, hogy válasszuk ki a kívánt telepítési formát.



Választhatunk a gyorstelepítés és a személyre szabott telepítés közül

Jelöljük be az *Expressz* választókapcsolót, és kattintsunk a *Telepítés* gombra.

Megjelenik a Windows XP 2. szervizcsomagjának *Végfelhasználói licencszerződése.*

Megjelenik a 2. szervizcsomag telepítővarázslója. Kattintsunk a *Tovább* gombra.

A telepítési folyamat elkészültével kattintsunk az *Újraindítás most* gombra, hogy a telepítést befejezzük.

A számítógép újraindul.

A telepítés után elsőként megjelenő ablak arra kér, hogy kapcsoljuk be az *Automatikus frissítések* szolgáltatást (megjegyzés: ha az Automatikus frissítések szolgáltatás beállítása jelenleg „A számítógéphez ajánlott frissítések automatikus letöltése és telepítése", nem jelenik meg ez a képernyő).

Az *Automatikus frissítések* bekapcsolásához – mint már láttuk – kattintsunk *A számítógép védelme az automatikus frissítési szolgáltatás azonnali bekapcsolásával (ajánlott)* lehetőségre, majd a *Tovább* gombra.

A 2. szervizcsomag telepítése ezzel befejeződött.

3.4 A szervizcsomag használata

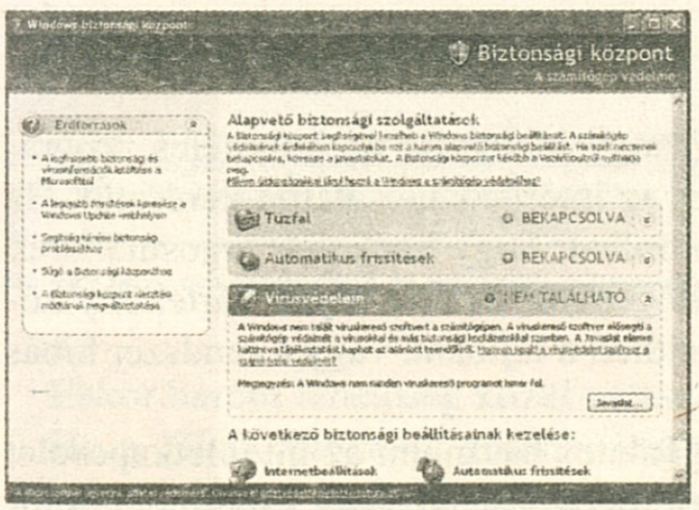
A Microsoft Windows XP 2. szervizcsomagjának telepítése után új és továbbfejlesztett szolgáltatások jelennek meg, ezek főbb elemeit a következőkben ismertetjük.

3.4.1 Windows Biztonsági központ

A *Windows Biztonsági központ* a számítógép pillanatnyi biztonsági állapotát jelzi, továbbá megjeleníti a számítógép biztonságosabbá tételéhez szükséges esetleges teendőket is.

A Windows Biztonsági központ megnyitásához válasszuk a *Start* menü *Vezérlőpult* parancsát.

A Vezérlőpulton kattintsunk a *Biztonsági központ* elemre.

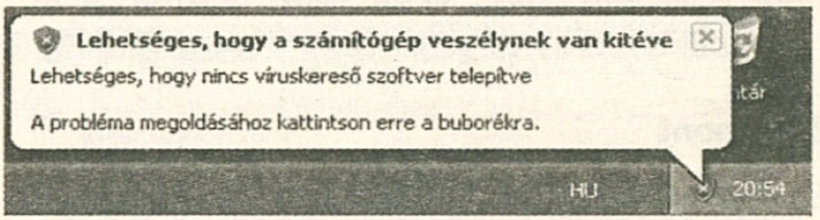


A Windows Biztonsági központ segítségével kezelhetjük az operációs rendszer biztonsági beállításait

A Windows Biztonsági központ a három alapvető biztonsági szolgáltatás állapotát jeleníti meg, ezek a *Windows tűzfal,* az *Automatikus frissítések* és a *Vírusvédelem.* Folyamatosan felderíti az esetleges problémákat, és értesítést küld, ha valami figyelmet igényel.

A Biztonsági központban továbbá gyorsan információhoz juthatunk a legújabb vírusokkal és a biztonsági fenyegetésekkel kapcsolatban, vagy biztonsági problémák esetén igénybe vehetjük a Microsoft ügyfélszolgálatának a segítségét. Bővebb információért csak kattintsunk az *Erőforrások* csoportban levő címsorok egyikére.

Amennyiben egy vörös pajzs, illetve a *Lehetséges, hogy a számítógép veszélynek van kitéve* üzenet jelenik meg az értesítési területen, a Windows Biztonsági központ ezzel figyelmeztet, hogy törődést igénylő biztonsági probléma adódott.



A Biztonsági központ üzenetben figyelmeztet az esetleges veszélyekre

A figyelmeztetésre kattintva megnyílik a Windows Biztonsági központ, így megtekinthetjük és módosíthatjuk az aktuális biztonsági beállításokat.

3.4.2 Windows tűzfal

A tűzfal azzal nyújt védelmet, hogy blokkolja az internetes programok hozzáférését a számítógéphez az internetkapcsolaton keresztül. Ha a tűzfal nincs bekapcsolva, előfordulhat, hogy hackerek jogosulatlanul megpróbálnak hozzáférni a számítógéphez, és arra olyan kártékony kódot telepítenek, amely megsemmisítheti a fájlokat, vagy a rendszer hibás működéséhez vezethet.

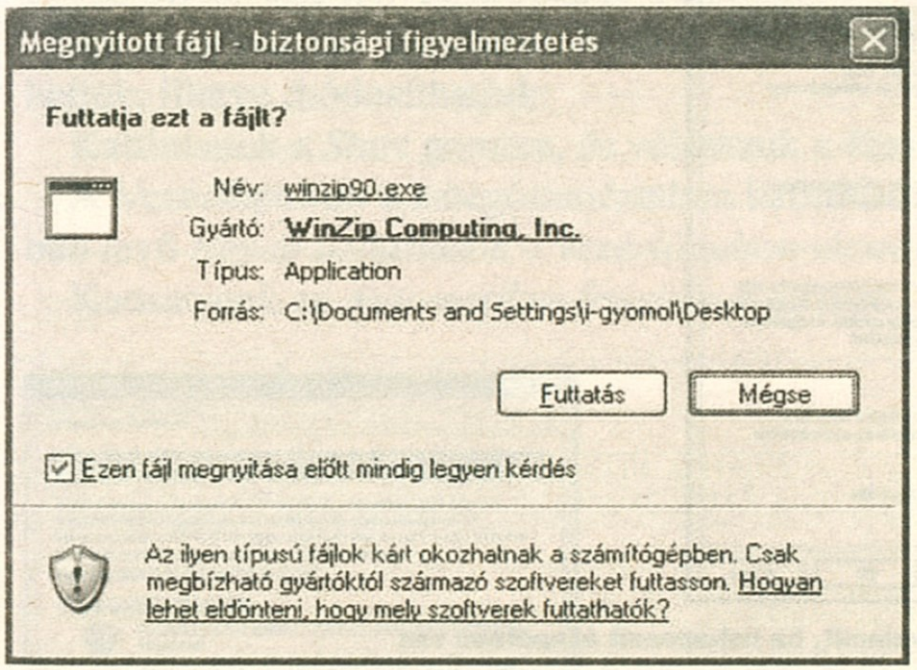
Tűzfalat általában mindenhol ajánlatos használni az internetkapcsolat típusától függetlenül, legyen az telefonos, ISDN- vagy kábelmodem, illetve digitális előfizetői vonal (DSL vagy ADSL).

Megjegyzés

A tűzfalas védelem nem kívánt velejárója, hogy a számítógépen futó programok számára is megtilthatja az internet elérését. Az internethez hozzáférni próbáló népszerű alkalmazások közé tartoznak az interneten át játszható és a többrésztvevős játékok, valamint bizonyos azonnali üzenetküldésre alkalmas programok.

Ahhoz, hogy számítógépünk még nagyobb biztonságban legyen, az új Windows tűzfal a 2. szervizcsomag telepítésének részeként bekapcsolt állapotú lesz.

A 2. szervizcsomag telepítése után, ha olyan programot futtatunk, amely megpróbál az internethez kapcsolódni, előfordulhat, hogy a Windowstól származó biztonsági figyelmeztetést kapuk. A riasztás közli, hogy a futtatott program megkísérel hozzáférni az internethez, és a Windows tűzfal blokkolta a próbálkozást.



Ha egy program megpróbál az internethez kapcsolódni, biztonsági figyelmeztetést kapunk

Ekkor három lehetőség közül választhatunk:

Ha a *Tiltás feloldása* gombra kattintunk, a programot felvesszük a Windows tűzfal *kivétellistájára,* így a program ekkor és a jövőben is hozzáférhet az internethez.

Ha a *Tiltás fenntartása* gombra kattintunk, a Windows tűzfal a későbbiekben is blokkolja a programot, így e program esetén többé nem jelenik meg a Windows biztonsági riasztás párbeszédpanel.

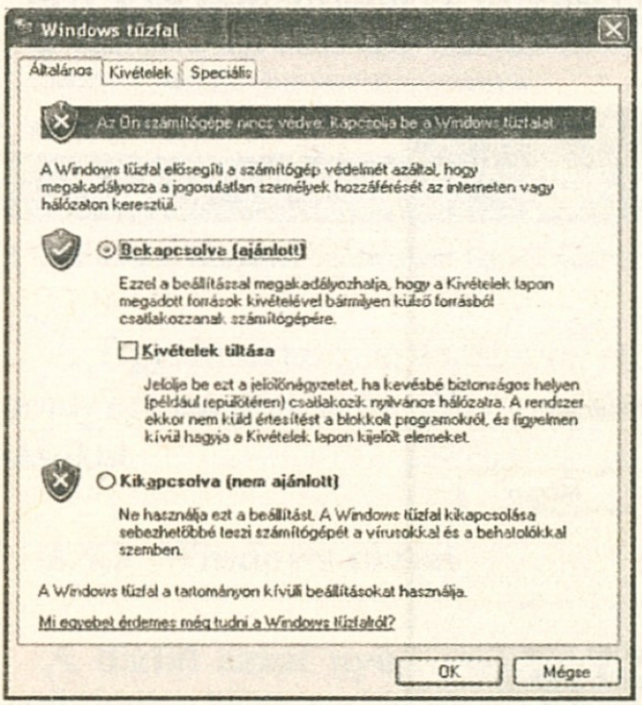
Ha a *Rákérdezés később* gombra kattintunk, a Windows tűzfal a későbbiekben is blokkolja a programot, és amennyiben a program kapcsolatot szeretne létesíteni, megjelenik a Windows biztonsági riasztás párbeszédpanel.

A Windows tűzfal beállításait a következőképpen ellenőrizhetjük és módosíthatjuk:

Kattintsunk a *Start* gombra, és válasszuk a *Vezérlőpult* parancsot.

A Vezérlőpulton kattintsunk a *Biztonsági központ* elemre.

A Biztonsági központ ablakának alsó részén kattintsunk a *Windows tűzfal* elemre.



A Windows tűzfal akkor ér valamit, ha bekapcsolt állapotban van

3.4.3 Vírusvédelem

A *vírusvédelmi* szoftverek megvédik a számítógépünket a legtöbb vírus, féreg és egyéb biztonsági fenyegetés ellen. Számos számítógépet előre telepített vírusvédelmi programmal látnak el, de arra is lehetőség van, hogy mi vásároljunk ilyet, majd telepítsük azt a számítógépünkre.

A vírusvédelmi program telepítése sajnos önmagában nem elég. Számítógépünk biztonságának megőrzéséhez a vírusvédelmi programot folyamatosan frissíteni kell.

A *Windows Biztonsági központ* felismeri a nagyobb gyártók által készített vírusvédelmi programokat. Biztonsági figyelmeztetés jelenik meg, ha a Windows nem talál telepített vírusvédelmi programot a számítógépen, vagy ha a felismert program nem naprakész.

3.4.4 Automatikus frissítések

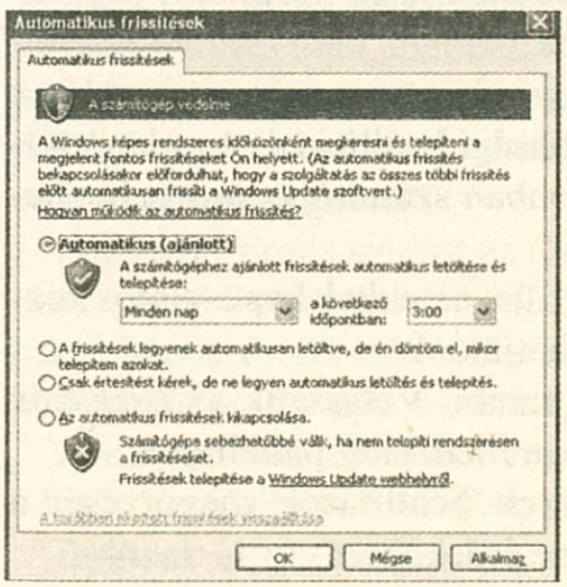
Az *Automatikus frissítések* szolgáltatás 2. szervizcsomagban található fejlesztései révén könnyen kiválaszthatjuk, mikor szeretnénk a legújabb frissítéseket letölteni és telepíteni, továbbá a telefonos kapcsolattal rendelkező felhasználók új technológiához jutnak a frissítések hatékonyabb letöltése érdekében. Ha még nem kapcsoltuk be az Automatikus frissítések szolgáltatást, a számítógépünk jóval sérülékenyebb a vírusokkal és egyéb biztonsági fenyegetésekkel szemben.

Az Automatikus frissítések beállításait a következőképpen ellenőrizhetjük, illetve módosíthatjuk:

Kattintsunk a *Start* gombra, és válasszuk a *Vezérlőpult* parancsot.

A Vezérlőpulton a kategórianézetben kattintsunk a *Lásd még* csoportban levő *Egyéb beállítások a Vezérlőpulton* elemre.

Kattintsunk az *Automatikus frissítések* elemre.



A Windows az általunk megadott időpontokban automatikusan letölti a biztonsági frissítéseket

Példánkban az Automatikus frissítések szolgáltatás bekapcsolt állapotú, ennek köszönhetően a Windows XP rendszeresen ellenőrzi a *Windows Update* webhelyet a letölthető legújabb frissítésekkel kapcsolatban, hogy megvédje számítógépünket a támadásoktól.

Ha az internethez kapcsolódunk, az Automatikus frissítések szolgáltatás ellenőrzi a fontos és a biztonsággal kapcsolatos frissítések elérhetőségét, és letölti őket. A frissítéseket letöltés után telepíteni kell a számítógépre, hogy érvénybe lépjenek. Az alapértelmezés szerinti beállítás *(Minden nap, 3:00)* azt jelenti, hogy az Automatikus frissítések szolgáltatás által letöltött frissítések valójában ebben az időpontban települnek a számítógépre, de a felhasználó ettől eltérő ütemezést is beállíthat.

3.4.5 Outlook Express

Számos vírust és férget e-mail üzeneteken keresztül küldenek. Bármilyen e-mail üzenet tartalmazhat a számítógépre vagy az azon tárolt adatokra nézve veszélyes vírust, még a látszólag ártalmatlan üzenetek is. A 2. szervizcsomag részét képező új mellékletkezelő alapértelmezés szerint csak a lehetséges veszélyforrásként számon tartott fájltípusok mellékletként való megnyitását tiltja le.

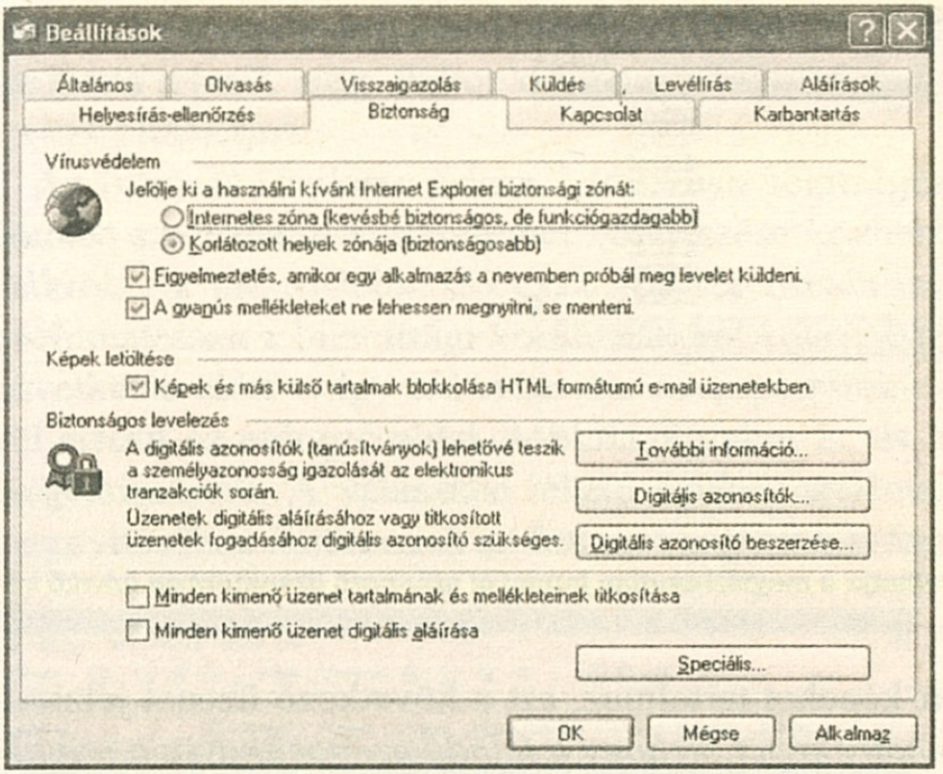
A Windows XP 2. szervizcsomagjának telepítését követően minden bizonnyal feltűnik majd, hogy néhány beállítás megváltozik. A Windows XP 2. szervizcsomagjában az *Outlook Express* programhoz tartozó alapértelmezett beállítások meggátolják az interneten keresztüli jogosulatlan hozzáférést a személyes adatainkhoz.

Az Outlook Express programban egyszerűen az egyéni igényekhez igazíthatók az elektronikus levelezés biztonsági beállításai. Az alapértelmezett beállítások megváltoztatásával azonban számítógépünk sebezhetőbbé válhat.

Az Outlook Express beérkezett e-mail üzenetekkel kapcsolatos biztonsági beállításait a következőképpen érhetjük el:

Nyissuk meg az Outlook Express programot. Válasszuk az *Eszközök* menü *Beállítások* parancsát, majd lépjünk a *Biztonság* panellapra.

A Microsoft javasolja az alapértelmezett beállítások megőrzését a számítógép és a személyes adatok védelme érdekében.



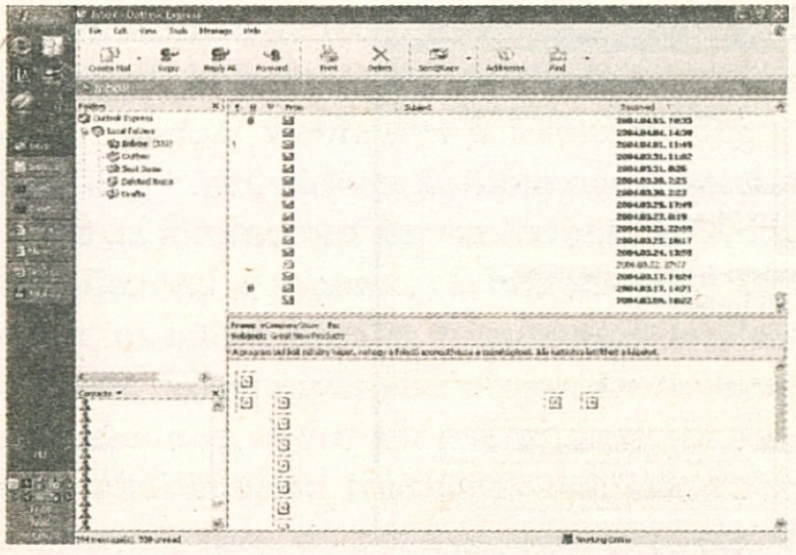
Az Outlook Express alapbeállításai kielégítő biztonságot nyújtanak a veszélyes küldemények ellen

A Windows XP 2. szervizcsomagjának egyik újításaként az Outlook Express hatékonyabban segít a levélszemét mennyiségének csökkentésében, mert megakadályozza a rosszindulatú levélküldők számára az e-mail címünk megszerzését. A kéretlen üzenetek és a szemétlevelek gyakran olyan képeket tartalmaznak, amelyek a küldő számítógépéről történő letöltés után jelennek meg. A képek letöltődésekor az üzenet küldője értesítést kap, és így megtudja, hogy az e-mail címünk valóban létezik és használatban van, tehát további kéretlen küldemények potenciális célpontjának tekinthető.

Alapértelmezés szerint az Outlook Express levélszemét elleni eljárása csak engedélyezésünket követően teszi lehetővé a külső forrásból származó képek és ábrák letöltését. Célszerű minden fogadott képet letiltani a megbízható forrásból származók kivételével.

A megbízható forrásból származó e-mail üzenetben szereplő képeket a következőképpen tekinthetjük meg:

Indítsuk el az Outlook Express programot, és nyissuk meg az adott e-mail üzenetet.



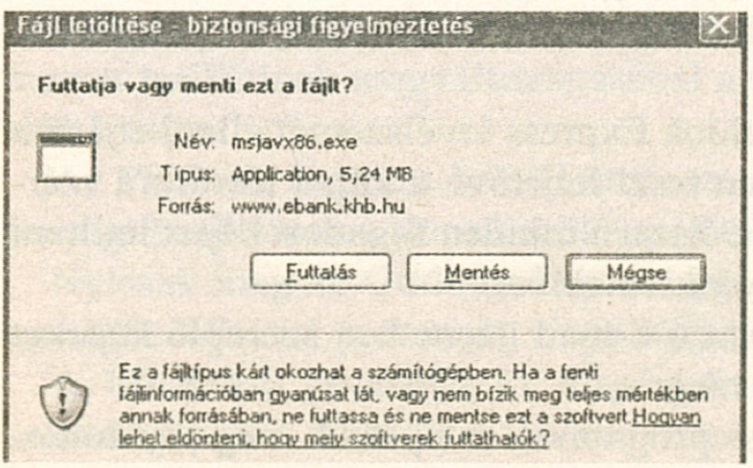
Az Outlook Express blokkolhatja a megbízhatatlan forrásból származó üzenetekben érkező képeket

Ha a levél letiltott képeket tartalmaz, ezt a következő üzenet jelzi: *A program blokkolt néhány képet, nehogy a feladó azonosíthassa a számítógépet. Ide kattintva letöltheti a képeket.*

Kattintsunk az üzenetsávra. A képek betöltődnek és megtekinthetjük őket.

3.4.6 Internet Explorer

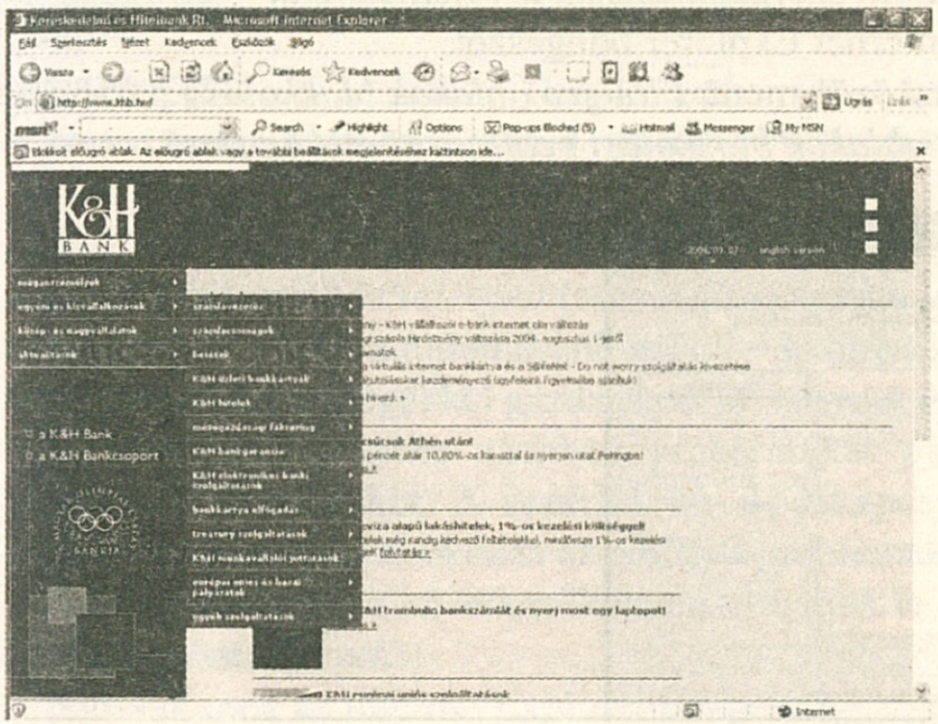
A 2. szervizcsomagban az *Internet Explorerhez* tartozó frissítések és kiegészítések között olyan alapértelmezés szerinti biztonsági beállítások szerepelnek, amelyek segítenek a lehetséges biztonsági fenyegetések azonosításában, és figyelmeztetnek velük kapcsolatban.



Fájl letöltésekor mindig biztonsági figyelmeztetést kapunk

Ha olyan helyre kattintunk, amely letöltést indít el, biztonsági figyelmeztetés jelenik meg. Ekkor kiválaszthatjuk, hogy a letöltést folytatjuk-e vagy elutasítjuk.

Az Internet Explorer *információs sávja* segítségével könnyebben tudomást szerezhetünk az internet böngészése közben előforduló problémákról. Az információs sáv csak szükség esetén jelenik meg, hogy figyelmeztessen a biztonsági kockázatokkal kapcsolatban – még azok bekövetkezte előtt –, így eldönthetjük, továbblépünk-e vagy sem. Ezenkívül értesít az előugró ablakok blokkolásakor is, és lehetőséget ad azok megtekintésére. A választási lehetőségeket tartalmazó legördülő menü megnyitásához kattintsunk az Internet Explorer információs sávjára.



Az Internet Explorer információs sávjában értesülhetünk az előugró ablakok blokkolásáról

Ha a *Blokkolt előugró ablak...* üzenetet látjuk, a következő lehetőségek közül választhatunk: *Előugró ablakok ideiglenes engedélyezése* (megtekinthetjük az adott előugró ablakot), *Webhely előugró ablakainak állandó engedélyezése* (az adott webhelyen levő előugró ablakok mindig megjelenhetnek), *Beállítások* (további lehetőségekért megnyitja az Előugró ablakok blokkolása párbeszédpanelt) és *Információs sáv — súgó* (többet megtudhatunk az információs sávról).

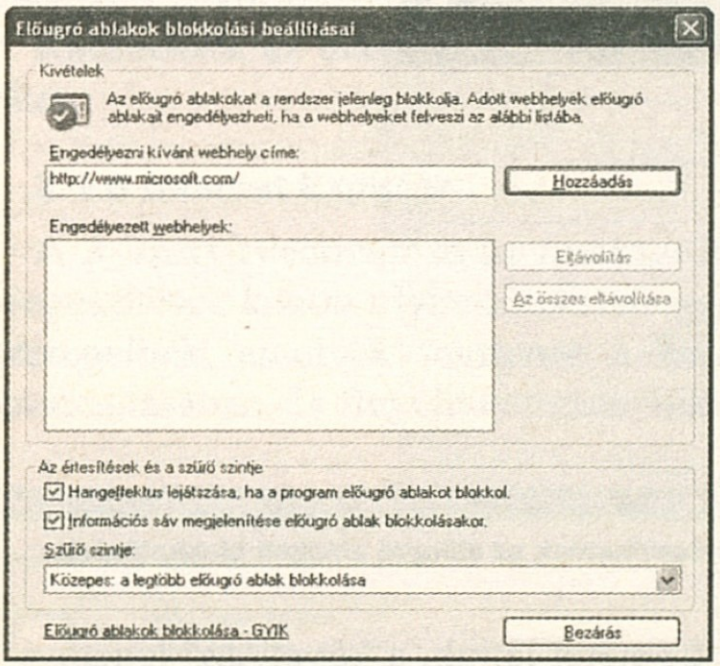
A 2. szervizcsomagban megtalálható az Internet Explorer előugró ablakokat blokkoló új szolgáltatása is, amely alapértelmezés szerint be van kapcsolva. Ezentúl a legtöbb esetben megakadályozható, hogy az engedélyünk nélkül jelenjenek meg előugró böngészőablakok.

Számos webhely – internetbank, kormányzati információs webhely, internetes újság – azonban gyakran használ előugró ablakokat az információk megjelenítéséhez. Ha rendszeresen látogatunk előugró ablakokat tartalmazó webhelyekre, felvehetjük őket a *kivétellistára.* Így ha bármikor felkeressük az adott webhelyet, az előugró ablakok akadály nélkül megjelennek.

Webhelyet a következőképpen vehetünk fel az Internet Explorer előugró ablakokat blokkoló szolgáltatásának kivétellistájára:

Nyissuk meg az Internet Explorer böngészőt.

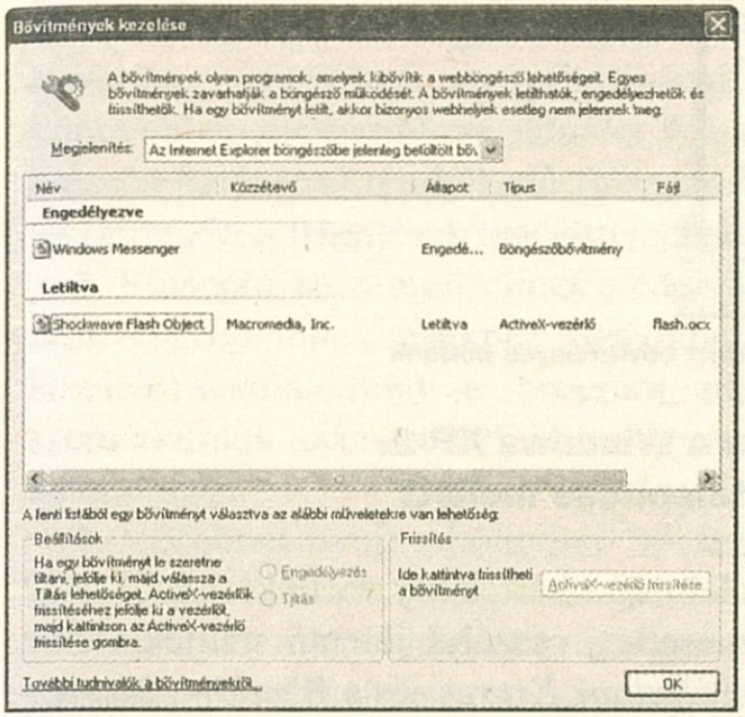
Kattintsunk az *Eszközök* menü *Előugró ablakok blokkolása* parancsára, majd az *Előugró ablakok blokkolási beállításai* menüpontra.



A kivétellistára felvett webhelyek akadálytalanul megjeleníthetnek előugró ablakokat

Az *Előugró ablakok blokkolási beállításai* párbeszédpanelen az *Engedélyezni kívánt webhely címe* mezőbe írjuk be a webhely teljes címét (például: **http://www.microsoft.com**).

Kattintsunk a *Hozzáadás,* majd a *Bezárás* gombra.



Az Internet Explorer bővítménykezelőjével engedélyezhetünk vagy letilthatunk bővítményeket

A 2. szervizcsomagban található másik új funkcióval letilthatjuk az Internet Explorer *bővítményeit* (másik elnevezésük *ActiveX-vezérlők*). A bővítmények – néha a tudomásunk nélkül – letöltött kis programok, amelyek további lehetőségekkel gazdagítják az Internet Explorer böngészőt.

A bővítmények néha azonban problémákat okozhatnak bizonyos programok futtatásakor. A vezérlők be- és kikapcsolásának lehetősége segít meghatározni, mi okozza az említett problémákat.

A bővítményeket a következőképpen tilthatjuk le az Internet Explorer *bővítménykezelőjével:*

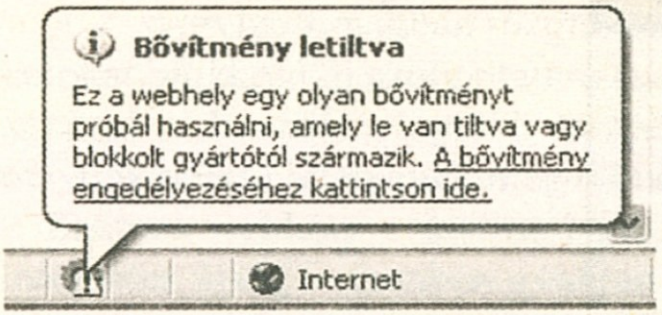
Nyissuk meg az Internet Explorer böngészőt.

Kattintsunk az *Eszközök* menü *Bővítmények kezelése* parancsára.

A *Bővítmények kezelése* párbeszédpanelen az *Engedélyezve* felirat alatt kattintsunk a kívánt bővítményre.

A *Beállítások* területen kattintsunk a *Tiltás,* majd az *OK* gombra.

Az Internet Explorer figyelmeztetést jelenít meg az értesítési területen, ha olyan webhelyre látogatunk, amelyhez a letiltott bővítmények egyike szükséges. A figyelmeztetésben szereplő hivatkozás az Internet Explorer bővítménykezelőjére mutat, így könnyen engedélyezhetjük a szükséges bővítményt.



Az Internet Explorer figyelmeztet, ha letiltott bővítménybe botlunk

3.5 A tíz legfontosabb érv a Windows XP 2. szervizcsomagjának telepítése mellett

1. Elősegíti a számítógép védelmét a kártékony mellékletektől. A 2. szervizcsomag figyelmeztet az esetleg veszélyt jelentő mellékletekre, így segít az *Internet Explorer,* az *Outlook Express* és a *Windows Messenger* programon keresztül terjedő vírusok elleni védekezésben.

2. Növeli a biztonságot a web böngészése közben. A 2. szervizcsomag által alkalmazott biztonsági beállítások megvédik a számítógépen tárolt és az Internet Explorer böngészővel letöltött fájlokat és tartalmat, így illetéktelenek nem férhetnek személyes adatainkhoz.

3. Elkerülhetjük a megbízhatatlannak tűnő fájlok letöltését. Az Internet Explorer letöltéseket nyomon követő funkciója és az Internet Explorer információs sávja figyelmeztet a potenciálisan veszélyes fájlok letöltése előtt, és e funkciók segítségével blokkolhatók a rosszindulatúnak ítélt fájlok.

4. Csökkenti a bosszantó előugró ablakok számát. Az Internet Explorer előugró ablakokat blokkoló szolgáltatása a kéretlen előugró hirdetések és más nem kívánt tartalom blokkolásával kellemesebbé teszi az internet böngészését.

5. Tűzfalas védelmet nyújt a rendszerindítástól a leállításig. A beépített, hatékony *Windows tűzfal* alapértelmezés szerint már rendszerindításkor működésbe lép. Ez segít megvédeni a Windows XP rendszert az interneten keresztül terjedő vírusoktól és férgektől.

6. Kézben tarthatjuk a biztonsági beállításokat. Az új *Windows Biztonsági központ* segítségével egyszerűen nyomon követhetjük a biztonsági rendszer állapotát, és a biztonsági beállítások egy helyen, kényelmes eszközökkel felügyelhetők.

7. Könnyedén elérhetjük a legújabb frissítéseket. A Windows XP *Automatikus frissítések* szolgáltatásának továbbfejlesztése révén még könnyebben elérhetjük az aktuális Windows-frissítéseket. Emellett a telefonos hálózattal rendelkező felhasználók számára új technológiát fejlesztettek ki a frissítések hatékonyabb letöltése érdekében.

8. Elősegíti az e-mail címek védelmét. Az Outlook Express programon végzett fejlesztéseknek köszönhetően csökkenthető a nem kívánt levelek száma, mert a program megnehezíti az esetleges levélszemétküldők számára azt, hogy meggyőződjenek e-mail címünk érvényességéről.

9. Védelmet nyújt a böngésző bővítményei okozta rendszerösszeomlások ellen. A Internet Explorer új *Bővítménykezelője* egyszerűvé teszi a bővítmények megtekintését és felügyeletét, így csökkenti a rendszerösszeomlások valószínűségét, és zavartalanabb böngészést tesz lehetővé.

10. Problémamentessé vált a vezeték nélküli hálózatok használata. A 2. szervizcsomagban továbbfejlesztették a vezeték nélküli hálózatok támogatását, így otthon és utazás közben egyaránt egyszerűbbé vált a vezeték nélküli hálózatok felismerése és a hozzájuk való csatlakozás.

4 Az SP2 optimális telepítése

A 2. szervizcsomag telepítésével megvédhetjük számítógépünket a webről ránk leselkedő különféle veszélyektől. Az előző fejezet részletesen bemutatta a telepítés pontos menetét. Ebben a fejezetben ismét a telepítés áll a középpontban: bemutatjuk azokat a módszereket és beállításokat, amelyekkel az egyéni felhasználók a legoptimálisabb módon telepíthetik az SP2-t.

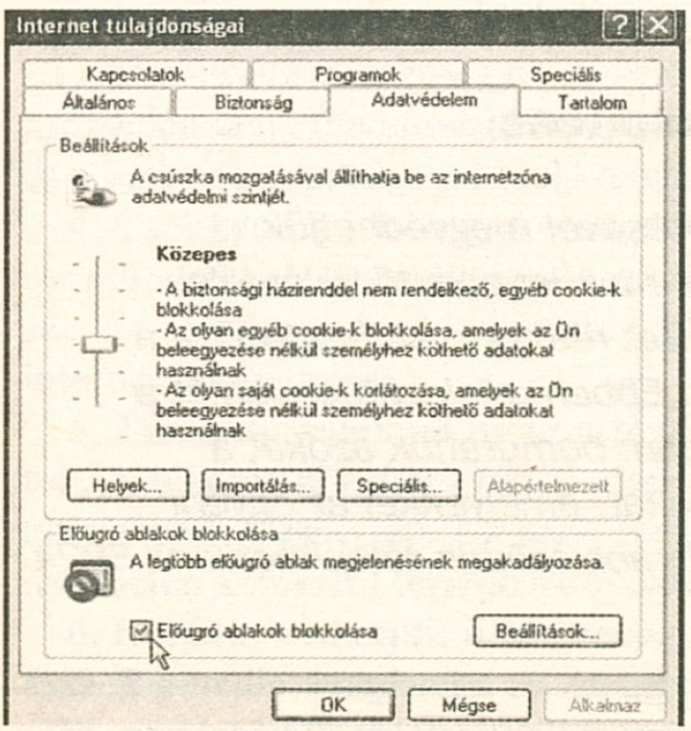
A *Microsoft* támadásba lendült a vírusok és a hackerek ellen: a 2. szervizcsomag (SP2) a „bugfix” gyűjtemény mellett egy sor új védelmi mechanizmust is tartalmaz. Nézzük, mit nyerünk ezekkel és hogyan működnek.

A 2. szervizcsomag kiadásával sok minden történt: az *Internet Explorert* újragenerálozták, az *Outlook Express* új képességeket örökölt nagy testvérétől, az *Outlooktól,* és a *Windows tűzfal* is sokkal kezelhetőbb lett. Mindent egybevetve: a Microsoft a 2. szervizcsomaggal teljesíteni látszik ama ígéretét, mely szerint több energiát invesztál a Windows biztonságába.

4.1 Reklámablakok blokkolása

Körkérdések eredménye igazolja: a popupok, amelyek már szinte minden kereskedelmi internetoldalon megtalálhatók, idegesítik a felhasználót. A 2. szervizcsomaggal a Microsoft a felhasználók kezébe adja az ellenszert: az *Internet Explorer 6*-ba egy popup-blokkolót integrált – nagy bosszúságára a reklámok készítőinek, akiknek a programjai ezáltal fölöslegessé válnak.

Így szabadíthatjuk meg a böngészőnket az előugró ablakoktól: a *Biztonsági Központban* válasszuk az *Internetbeállítások* pontot, majd pipáljuk ki a *Előugró ablakok blokkolása* jelölőnégyzetet.



Előugró ablakok blokkolása: az Internetbeállítások ablakban pipáljuk ki a megfelelő jelölőnégyzetet

Ennek azonban megvan az a hátránya, hogy az érdekes popupok sem jelennek meg többé. Ezért nyissuk meg az *Eszközöket,* majd az *Előugró ablakok blokkolását,* végül a beállításokat. Itt adhatunk meg kivételeket a szabály alól. Írjuk be a domaineket, amelyekről engedélyezni akarjuk a popupokat, és kattintsunk a *Hozzáadás* gombra. Amennyiben a szűrő szintjét *Az összes előugró ablak tiltására* állítjuk, minden lehetséges ablak megjelenését megakadályozzuk, még az olyanokét is, amelyek csak külön szándékos egérkattintásra nyílnak meg, mint a reklámbannerek.

Tipp

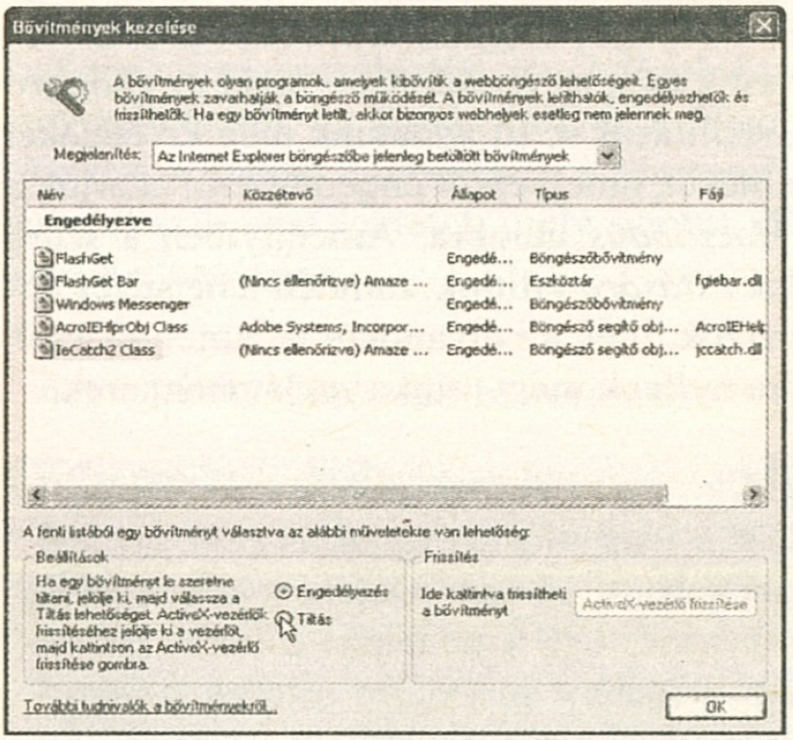
Tegyünk a Beállítások alatt pipát a Hangeffektus lejátszása elé. Így minden blokkolt ablakról hangjelzést kapunk, és nem maradunk le az esetleg fontos információkról a weboldalakon. Egy kattintással a popup ikonra jobbra lent az Internet Explorerben eljutunk az Előugró ablakok kezeléséhez, ahol engedélyezni vagy tiltani tudjuk a popupokat.

4.2 Bővítmények kezelése

Sok program – kérve vagy kéretlenül – hozzáadódik az *Internet Explorerhez.* Ezek közé tartozik például a *Windows Messenger,* az *ICQ,* a *Google eszközsor* vagy a *Macromedia Flash.* Spyware-ek, mint például az *Alexa* plugin is, észrevétlenül a böngészőre akaszkodhatnak. Most, a javított bővítménykezelővel teljes áttekintést kapunk ezekről. Ebben a plugineket egyetlen kattintással, nagyon gyorsan és kényelmesen tudjuk az Internet Explorerből eltávolítani vagy hozzáfűzni. A kezelőt teljes áttekintéssel minden előforduló vendégprogramról az *Eszközök* menü *Bővítmények kezelése* pontja alatt találjuk.

Valamivel jobb a strukturált nézet, amely ugyanitt, *Az Internet Explorer böngészőbe jelenleg betöltött bővítmények* alatt aktiválható. A bővítmények itt szét vannak osztva Aktívakra és Tiltottakra. Válasszuk ki a lista egyik elemét, és tegyünk pipát a *Tiltás* elé, ezzel az illető bővítményt kikapcsoljuk.

Ha egy *ActiveX*-modulról van szó, csak az *Alkalmaz* gombra kell kattintanunk, hogy a böngészőt az aktuális állapotra hozzuk. Minden másnál újra kell indítani az Internet Explorert.



A bővítménykezelőben gombnyomásra letilthatjuk a Internet Explorerre akaszkodó bővítményeket

Tipp

Először kapcsoljunk ki minden bővítményt, amelyet nem tudunk egyértelműen azonosítani, és csak igény esetén kapcsoljuk őket vissza. Így javítunk a biztonságon és erőforrást takarítunk meg.

4.3 Az Internet Explorer biztonságossá tétele

Több mint 90 százalékos piaci részesedésével az *Internet Explorer* a legelterjedtebb webböngésző, és mint ilyen, a hackertámadások kedvelt célpontja. Nyissuk meg a biztonsági beállításokat az *Eszközök* menü *Internetbeállítások* pontja alatt.

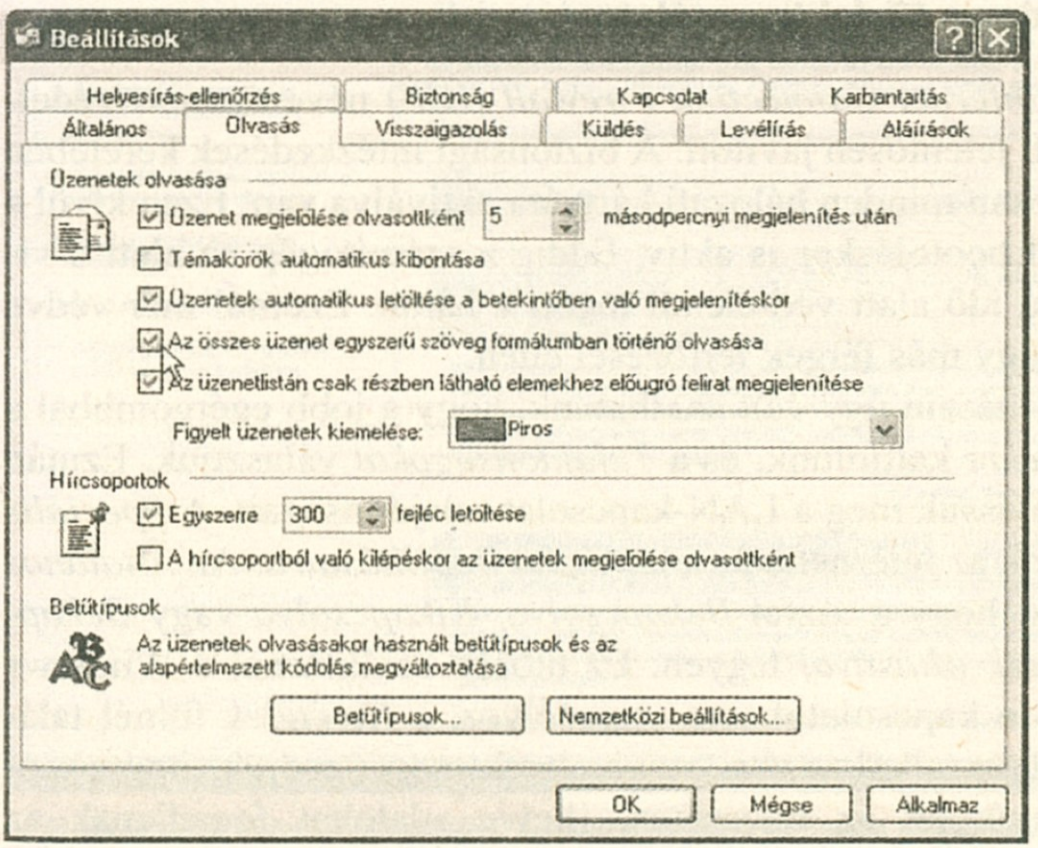
A *Zóna biztonsági szintjénél* (Egyéni szint) új beállítás a *Fájlok megnyitása fájlkiterjesztés helyett tartalom alapján.* Ez hivatott leleplezni például azt, ha egy trójai képnek álcázza magát. Az intranetbiztonság szempontjából egy további lépést jelent a helyes irányba az a lehetőség, hogy a helyi hálózathoz biztonsági zónát lehet konfigurálni. Így sok hackertámadást eleve kizárhatunk.

Tipp
Kattintsunk a Biztonság fülnél az Egyéni szintre, és válasszuk ki a közepeset. Itt a biztonsági óvintézkedések megfelelően szigorúak.

4.4 E-mailek biztonságos olvasása

Az internetről érkező email-férgek elleni küzdelemhez a Microsoft olyan új védelmi mechanizmusokat nyújt az *Outlook Expressben,* amelyek eddig csak „nagy testvérnél", az *Outlooknál* álltak rendelkezésre. Bár a Microsoft még mindig nem épített be spamszűrőt, most legalább már meg lehet jeleníteni az e-maileket általánosan csak szövegként, és nem HTML-ként. Így a szkriptek, amelyek eddig automatikusan lefutottak, először egyáltalán nem aktiválódnak.

Menjünk az *Eszközök* alatt a *Beállításokra,* majd válasszuk az *Olvasás* fület, és tegyünk pipát az *Összes üzenet egyszerű szöveg formátumban történő olvasása* elé.



Most már meg lehet jeleníteni az e-maileket szöveges formátumban

Ha egy e-mailt mégis inkább HTML formátumban akarunk megnézni, kapcsoljuk be a *Nézet* alatt az *HTML formátumú üzenet* beállítást, vagy nyomjuk le az **Alt + Shift + H** billentyűkombinációt. További biztonsági intézkedés az a lehetőség, hogy a képek automatikus letöltését külső forrásokból kikapcsolhatjuk. A spamküldők ugyanis gyakorlatilag láthatatlan, egy pixel méretű képekbe linkeket építenek be. Ezeket a tartalommal együtt letöltjük, és így meg tudják állapítani, hogy az e-mail fiókunk még aktív-e. Ha egy e-mail ilyen képeket tartalmaz, azonnal figyelmeztetés jelenik meg a képek blokkolásáról. Ha vannak olyan objektumok, amelyeket látni szeretnénk, ezeket az e-mail fejlécében rendelkezésre álló mezőre kattintva utólag betölthetjük.

Tipp

Ha a képeket továbbra is azonnal szeretnénk betöltetni, egy kicsit elrejtve, Eszközök / Beállítások alatt, a Biztonság fülnél megtaláljuk a Képek blokkolása beállítást, ezt kell feloldani hozzá.

4.5 A Windows tűzfal használata

A korábban *Internet Connection Firewall (ICF)* néven ismert védelmen a Microsoft jelentősen javított. A biztonsági intézkedések keretében a tűzfal általánosan minden hálózati kártyára aktiválva van. Ezen kívül a Windows tűzfal bootoláskor is aktív. Eddig a számítógép ez alatt a viszonylag hosszú idő alatt védtelenül lógott a hálón. Ezentúl már védve lesz a *Blaster* vagy más férgek fertőzései ellen.

A tűzfal beállításain úgy változtathatunk, hogy a jobb egérgombbal a *Hálózatok helyekre* kattintunk, és a *Tulajdonságokat* választjuk. Ezután jobb gombbal nyissuk meg a LAN-kapcsolat tulajdonságait. A *Speciális* fülnél kattintsunk az internetkapcsolat tűzfal *Beállításaira.* Az *Általános* fülnél rögzítsük, hogy a tűzfal *Bekapcsolva, Kikapcsolva* vagy *Bekapcsolva / Kivételek tiltásával* legyen. Ez utóbbi beállításnál a Windows tűzfal semmilyen kapcsolatot sem engedélyez, a *Kivételek* fülnél találunk minden olyan alkalmazást, amelyeknek megengedjük, hogy kapcsolatot építsenek fel az interneten, illetve adatokat fogadjanak az internetről. Ha egy eddig ismeretlen alkalmazás próbál meg kapcsolatot

létesíteni, a Windows tűzfal megkérdezi, hogy engedélyezzük-e. Ezt a jellemzőt már ismerjük más személyi tűzfalakból, mint amilyen például a *ZoneAlarm* vagy a *Symantec Firewall.*

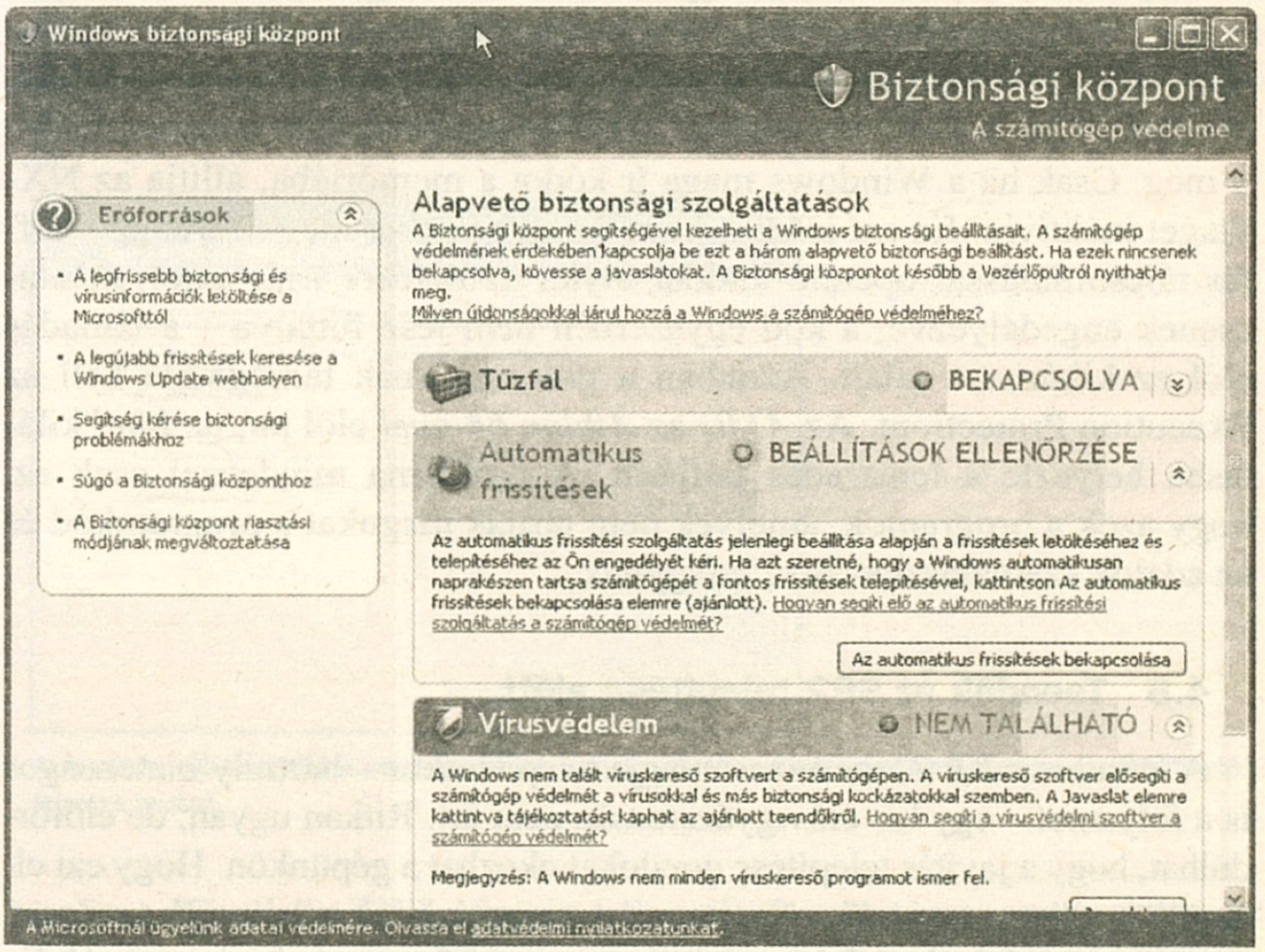
Tipp

Aki csak a tűzfalat használja, és nélkülözni tudja a ZoneAlarm és társai extráit, annak elegendő az ingyenes Windows tűzfal.

TiPP PLUSZ

4.6 Biztonsági segédprogramok kezelése

Az új Windows *Biztonsági központban* a Microsoft minden fontos segédprogramot egyesít. Itt találjuk a *Windows tűzfalat,* az *Automatikus Windows frissítést,* sőt a *vírusvizsgálónkat* is.



Az új Biztonsági központ elnevezésű konzolról minden lényeges biztonsági elem elérhető

Utóbbi nem a Microsofttól jön, és ahhoz, hogy a Windows felismerje, egy meghatározott portra kell irányulnia. Ha ez nem stimmel, a Windows XP hibásan azt üzeni, hogy nincs telepített vírusölő. Idegen tűzfalakat is csak akkor ismer fel a Biztonsági központ, ha ezt az interfészt használják. Remélhetőleg a jövőben minden gyártó támogatni fogja ezt a munkakönnyítő eszközt.

A Biztonsági központot pajzs ikon formájában megtaláljuk a *Tálcán,* az óra mellett. Ha a Windows XP-s számítógép egy domainbe van bejelentkezve, nincs Biztonsági központ. A Microsoft feltételezi, hogy egy domainben a rendszergazda őrködik a számítógép biztonsága felett, ezért ez az intézkedés értelmetlen volna.

4.7 Futtatásvédelem

A 2. szervizcsomaggal a Windows XP *futtatásvédelmet* is kap *(Execution Protection).* Ez alapvetően megakadályozza a programkódok indítását. Ehhez a teljes memóriát *NX-Flaggel* (NX=„No execute") jelöli meg. Csak ha a Windows maga ír kódot a memóriába, állítja az NX-Flaget inaktívra. Ez azt jelenti, hogy ha egy hacker megkísérel egy puffer túlcsordulással operáló kóddal olyan területekre írni, amelyek nincsenek engedélyezve, a kód egyszerűen nem lesz futtatva – a támadás alól ez kihúzza a talajt. Azonban a processzornak támogatnia kell az Execution Protectiont. Az *AMD* az *Athlon 64-gyel* elöl jár, az *Intel* kilátásba helyezte a lemaradás pótlását. A probléma mindezzel csak az, hogy azok a programok, amelyek nem tartják magukat a programkód és az adatok szétválasztásához, lefagynak.

4.8 Teendők az SP2 telepítése előtt

A Windows XP 2. szervizcsomagja telepítésekor – bármily biztonságos is a folyamat – egy kis elővigyázatosság nem árt. Ritkán ugyan, de előfordulhat, hogy a javítás telepítése gondokat okozhat a gépünkön. Hogy ezt elkerüljük, illetve megelőzzük, nem árt megszívlelni néhány jó tanácsot. Legelőször is készítsünk biztonsági mentést létfontosságú adatainkról. Ez talán hosszadalmas művelet, de megéri: ha mégis beüt a mennykő, adata-

inktól nem kell örökre búcsút vennünk. Ideiglenesen kapcsoljuk ki vagy távolítsuk el a szoftveres tűzfalat és a vírusirtó szoftverünket a telepítés előtt. Sokak ütköznek problémába a telepítés során, mert elfeledkeznek erről. Sok keserűséget, felesleges gondot okozhat, ha ezt nem tesszük meg – többet, mint azt sok tapasztalt PC felhasználó képzeli. Miután a telepítés befejeződött, kapcsoljuk vissza biztonsági szoftvereinket.

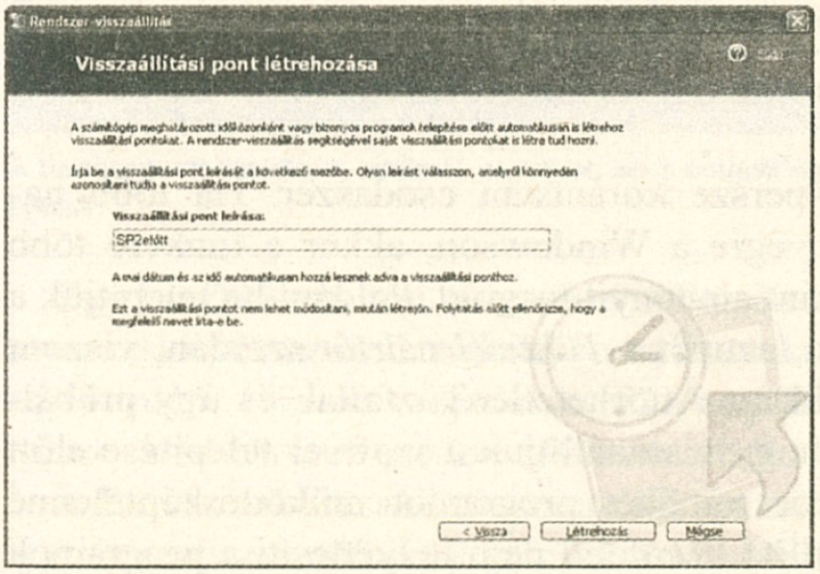
Ellenőrizzük a merevlemezünket a lemezhibák szempontjából. Az XP-ben ez a *chkdsk /f* parancssori futtatását jelenti (*Start/Futtatás*). A művelet végrehajtásához újra kell indítanunk a gépet.

Hozzunk létre egy rendszer-visszaállítási pontot (alább megmutatjuk hogyan)!

Zárjunk be minden felesleges alkalmazást!

Ezek után nézzük, hogy hozhatunk létre rendszer-visszaállítási pontot.

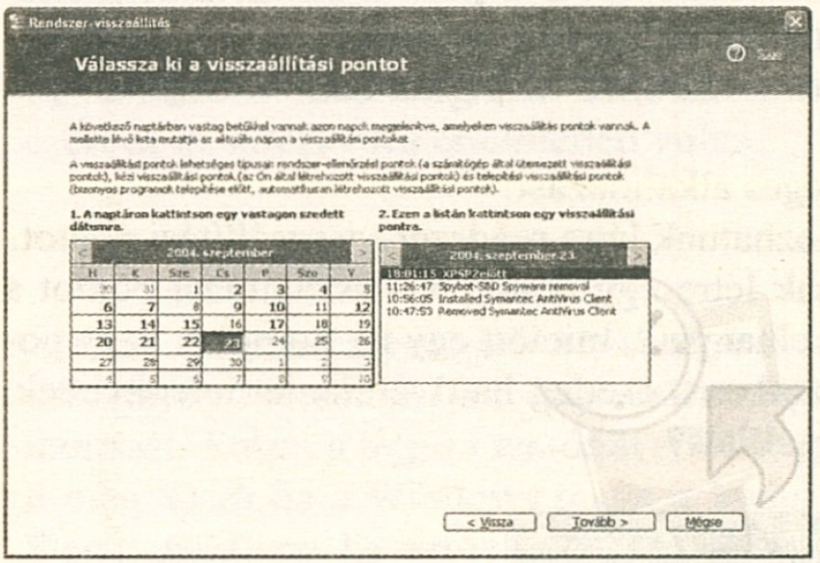
Az a tanács, hogy hozzunk létre egy rendszer-visszaállítási pontot a Windows XP-ben, gyakorta elhangzik, mielőtt egy új, komplex vagy potenciálisan problematikus szoftvert, esetleg hardverelemet telepítenénk. De mi is az a rendszer-visszaállítás?



A rendszer-visszaállítási pontnak olyan nevet adjunk, amely később könnyen azonosítható állapotra mutat

Ez a Windows XP-be épített helyreállító szisztéma, amely automatikusan, naponta „pillanatfelvételeket" készít a Windows rendszerfájljairól, így később visszaállíthatunk egy olyan korábbi állapotot, amikor

még minden rendben működött. Igaz, hogy általában az automatikusan mentett visszaállítási pontra is támaszkodhatunk (feltéve, hogy ez a funkció be van kapcsolva), mégis sokkal praktikusabb, ha mi magunk hozunk létre egy-egy ilyen mentést, amelyet azután úgy nevezünk el (például *ZoneAlarm Pro 5.1 telepítése előtt),* hogy később könnyedén azonosítani tudjuk. Így szükség esetén egyértelmű lesz, melyik mentési pontot kell használnunk.

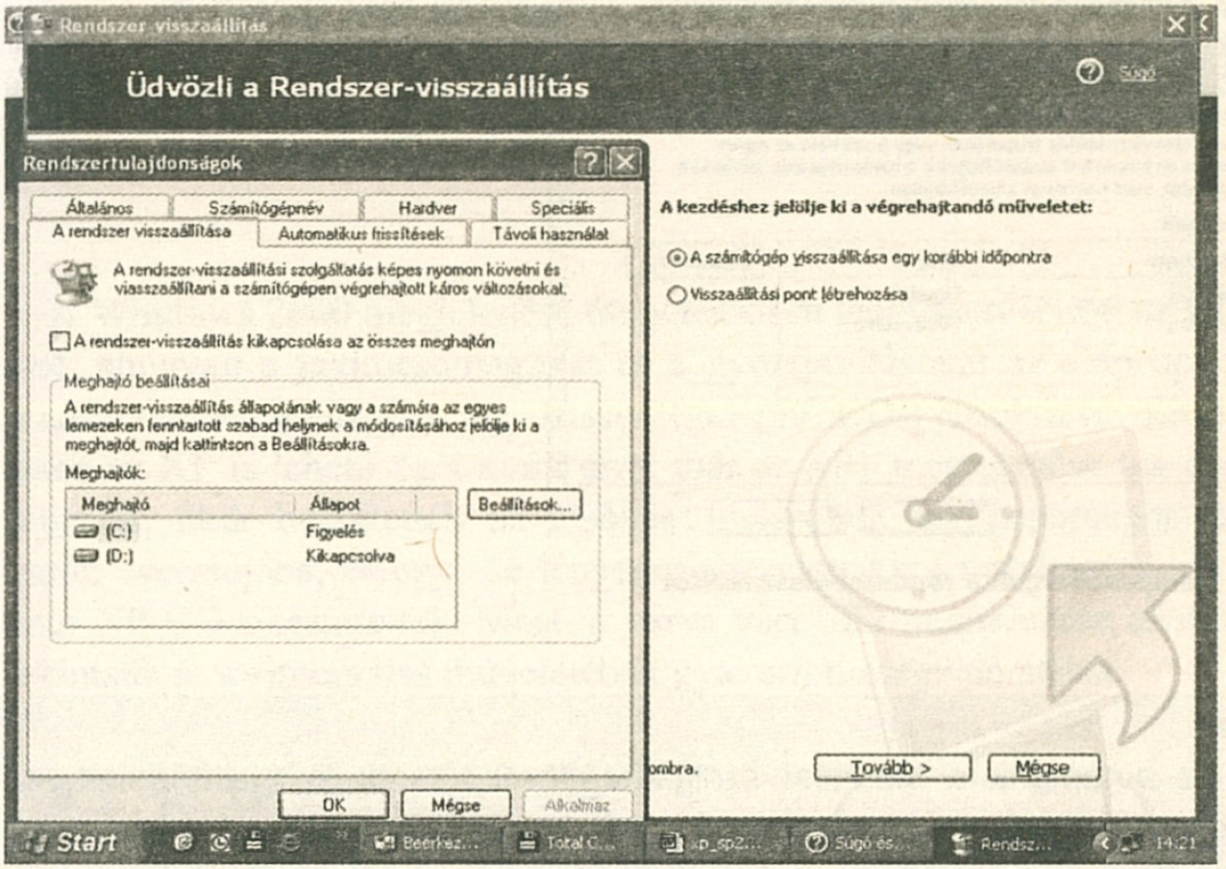


A rendszer-visszaállítási pontokhoz mindig dátum, percre pontos időpont és név fűződik

A rendszer-visszaállítás persze korántsem csodaszer. Ha több nagyobb változtatást hajtunk végre a Windowson, akkor e funkció több problémát okozhat annál, mint amennyit megold. Például ha telepítjük a *ÁttörhetetlenTűzfalat* hétfőn, azután a *TökösVírusírtót* szerdán, viszont csütörtökön probléma adódik az ÁttörhetetlenTűzfallal, és úgy próbáljuk orvosolni a problémát, hogy visszaállítjuk a szoftver telepítése előtt kreált mentési pontot, akkor mindkét programot működésképtelenné tesszük. A rendszer-visszaállító ezenfelül nem helyettesíti a programok eltávolítását. Minden olyan programot el kell távolítanunk, amelyet az általunk visszaállítandó mentési pont után hoztunk létre.

Rendszer-visszaállítási pont létrehozásához nyissuk meg a *Rendszer-visszaállítás varázslót:* kattintsunk a *Start* menü *Súgó és támogatás* parancsára. Ezután válasszuk a *Teljesítmény és karbantartást,* majd a *Módosítások visszavonása a rendszer-visszaállítási szolgáltatással* opciót,

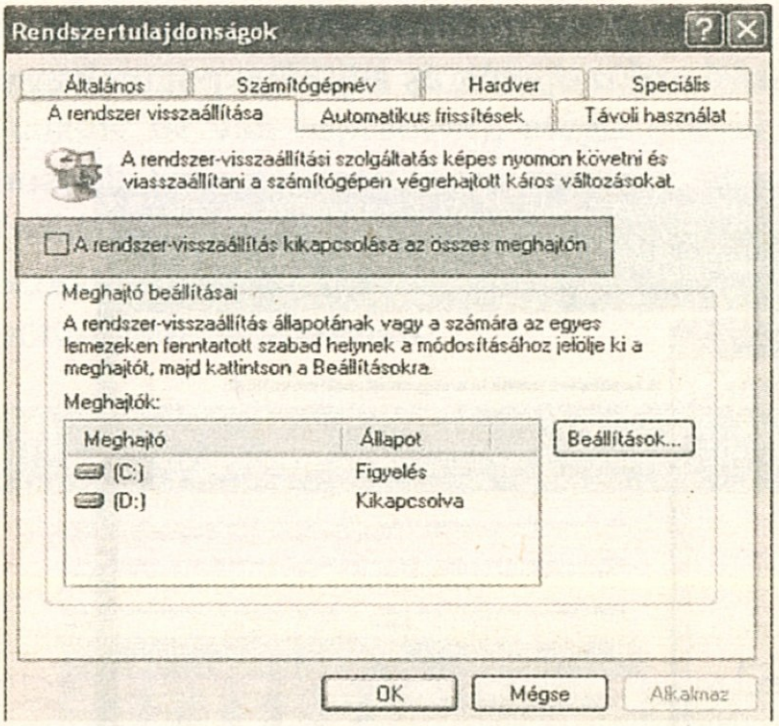
végül pedig *A Rendszer-visszaállítás varázsló használata* elemet. Itt válasszuk a *Visszaállítási pont létrehozása* opciót, és adjunk a pontnak egy könnyen azonosítható nevet.



A Rendszer-visszaállítás varázsló segíthet, ha a dolgok egy-egy telepítés után összekuszálódnának

Egy korábbi mentési pont visszaállításához indítsuk el hasonlóképpen a varázslót, és az első képernyőn válasszuk *A számítógép visszaállítása egy korábbi időpontra* opciót, majd a naptáron válasszuk ki a kívánt dátumot (a félkövéren szedett dátumok jelzik, mikor történt a mentés).

A Rendszer-visszaállítót sokan kikapcsolják, egyfelől azért, mert helyet és rendszererőforrást igényel a működéséhez, esetenként pedig más okból (például vírusok eltávolításánál). A funkció ki- vagy bekapcsolásához kattintsunk a *Start* menüre, majd a *Vezérlőpultra,* ahol keressük meg a *Rendszer* ikont. A megnyíló ablakban válasszuk *A rendszer visszaállítása* fület, ahol megtaláljuk a rendszer ki- vagy bekapcsolására szolgáló jelölőnégyzetet (a szolgáltatás aktiválásához legalább 200 Mbájt szabad lemezterülettel kell rendelkeznünk).



Ki- és bekapcsolhatjuk a rendszer-visszaállítót

Info

Ha az automatikus frissítési szolgáltatásával töltünk le frissítéseket, a rendszer-visszaállítás a szoftverfrissítés telepítése előtt létrehoz egy visszaállítási pontot. Ha elemeket töltünk le, de nem telepítjük azokat, nem jön létre visszaállítási pont. Visszaállítási pont csak az összetevők telepítésének a megkezdésekor keletkezik. Korszerű telepítőkkel ellátott szoftverek telepítése esetén is automatikusan létrejön egy új visszaállítási pont.

5 Az SP2 integrálása az XP telepítőlemezébe

Kevesen tudnak róla, de az SP2-t úgy is beágyazhatjuk az XP operációs rendszerbe, hogy létrehozunk egy új, SP2-vel kiegészített XP telepítőlemezt. Ennek előnyeit talán felesleges is ecsetelni: azzal ugyanis, hogy már telepítéskor ott vannak a javítások a rendszerben, nagy súly kerül le a vállunkról. Hiszen így a telepítés után az

egyébként kötelező (!) frissítési procedúra nagy része elmaradhat – amikor a netre lépünk, gépünk már a legtöbb vonatkozásban védve lesz a külső veszélyektől, továbbá rengeteg időt spórolunk. A vállalatoknál is rengeteget könnyít a felelősök életén az, ha a Windowst már közvetlenül az SP2-vel együtt telepíthetik az alkalmazottak gépeire.

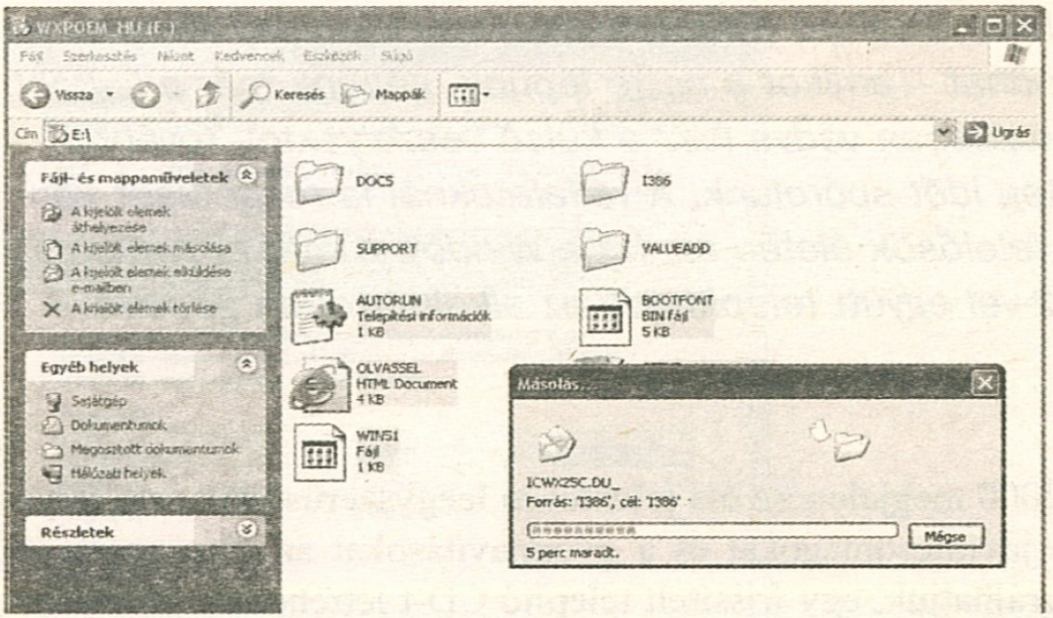
A Windows 2000 megjelenése óta jelentősen leegyszerűsödött az a folyamat, ahogyan a javítócsomagokat és a gyorsjavításokat az alap operációs rendszerbe integrálhatjuk, egy frissített telepítő CD-t létrehozva. Természetesen az XP is lehetőséget nyújt erre: már az SP1 megjelenése óta akadtak olyanok, akik beépítették az elsőként megjelent javítócsomagot az XP „szűz" verziójába, és egy – e lényeges szervizpakkot tartalmazó – bootolható XP CD-t készítettek. Most, a várva várt SP2 megjelenése alkalmával tekintsük át az integrálás műveletének gyakorlati megvalósítását.

5.1 Az XP SP2 beszerzése

Az előző fejezetekben már részletesen bemutattuk a 2. szervizcsomag beszerzésével kapcsolatos tennivalókat. Ezek röviden a következők. Először is töltsük le az internetről az XP SP2 magyar (vagy kívánt nyelvű) verzióját, vagy másoljuk ki a birtokunkban lévő XP SP2 CD-ről. Hozzuk létre az *sp2* mappát a gyökérkönyvtárban *(c:\sp2)*, és helyezzük bele a javítócsomagot. Miután ezzel kész vagyunk, nevezzük át a fájlt későbbi teendőink megkönnyítése végett *xpsp2.exe-re*.

5.2 Az XP másolása a merevlemezre

Második lépésként hozzuk létre a merevlemezünkön az xp nevű mappát a gyökérkönyvtárban *(c:\xp)*, majd fogjuk a Windows XP telepítőlemezünket, és másoljuk a CD tartalmát az újonnan készített könyvtárba.



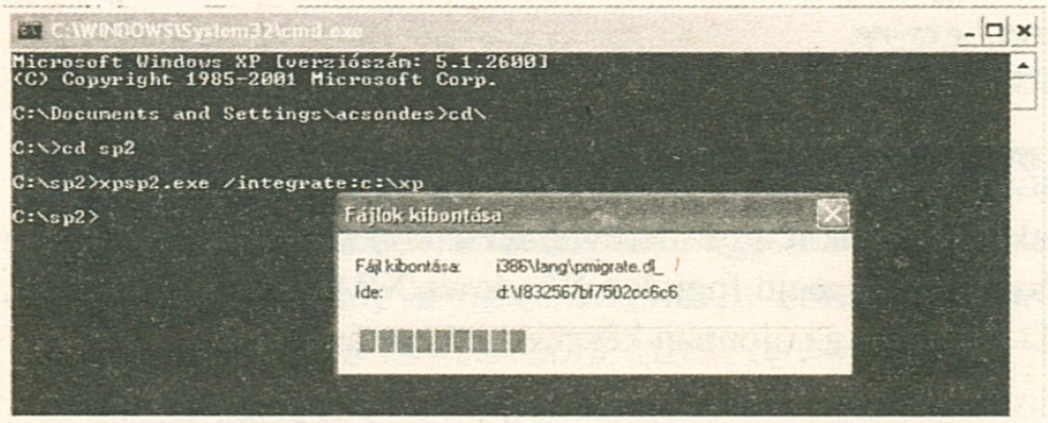
Második lépés: költöztessük az XP CD-t a merevlemezre

5.3 Az SP2 integrálása az XP-be

Nyissuk meg a parancssort a *cmd* paranccsal *(Start/Futtatás/cmd)*. A parancssorban gépeljük be a következőt (mindegyik sor után leütve az *Entert*):

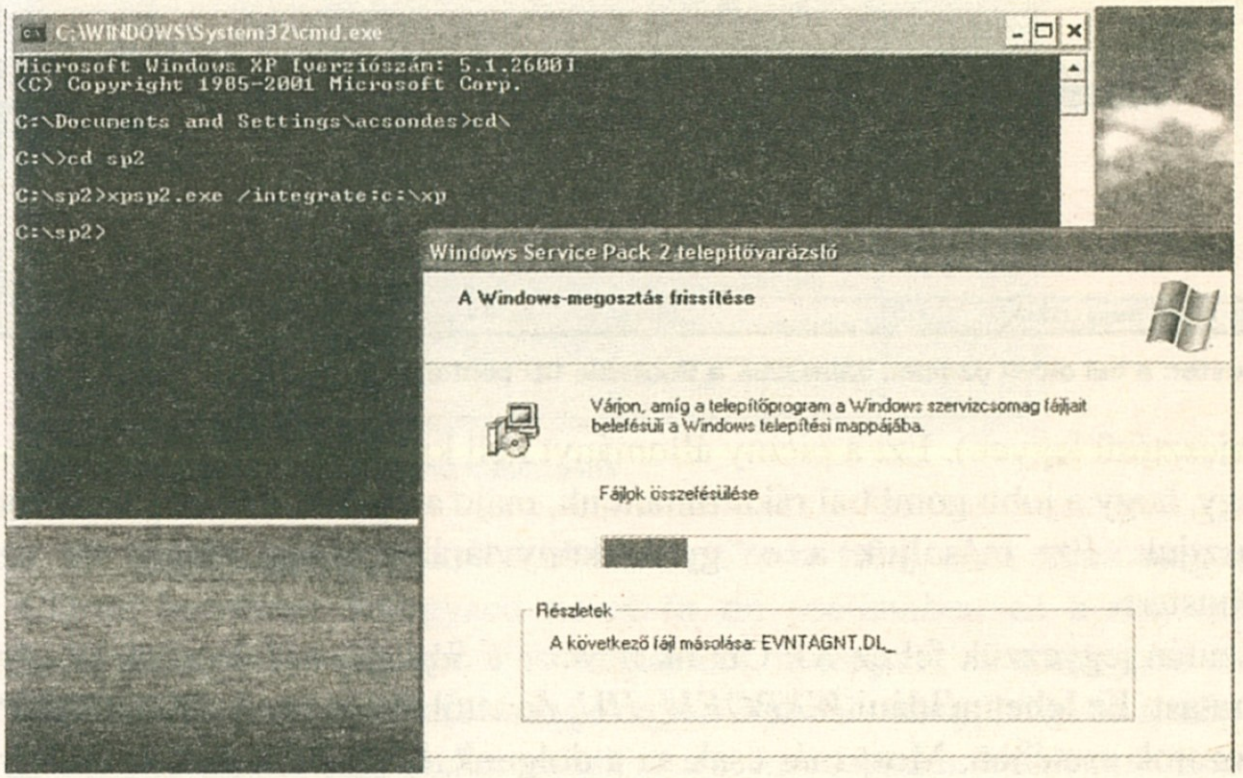
```
cd\
cd sp2
xpsp2.exe /integrate:c\xp
```

Ekkor megindul az *integrálás* folyamata. Először megtörténik a fájlok kicsomagolása az xpsp2.exe-ből.



Önkicsomagolás: Az integrálás első mozzanata a fájlok kibontása

Ezután végbemegy az SP2 beépülése az alap XP-be. A művelet végén egy kis ablak tájékoztat arról, hogy az integrált telepítés sikeresen befejeződött.



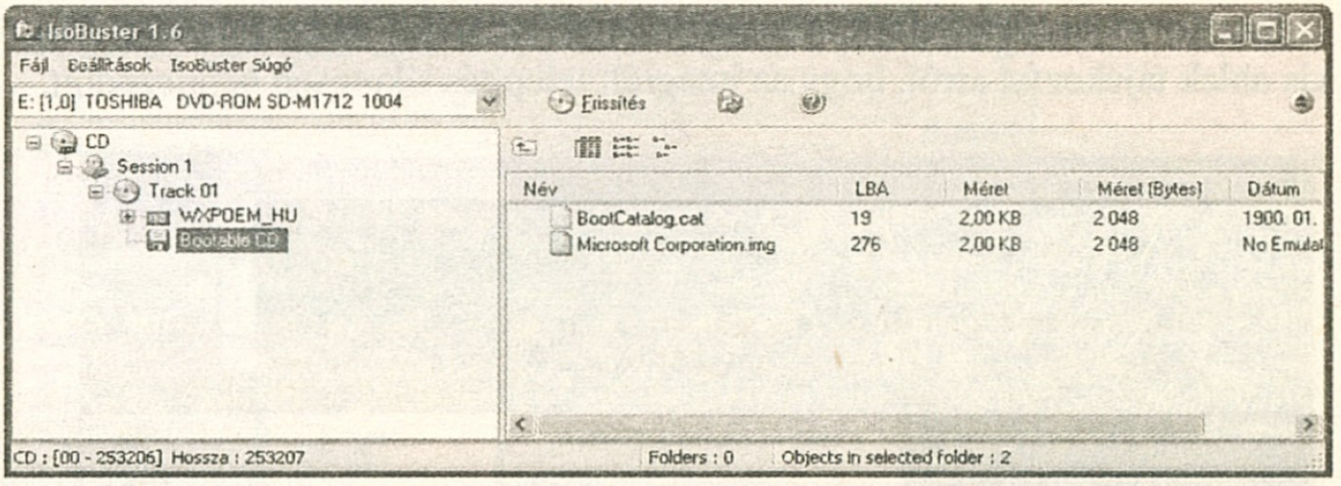
Összefésülés: az SP2 beépül az XP-be

5.4 A lemez bootolhatóvá tétele

A következő lépés már egy kicsit kacifántosabbnak ígérkezik. Ugyanis hiába épült be az SP2 az XP-nkbe, még ne írjuk ki a lemezt – ugyanis az így még nem lesz bootolható. Hogy ezt lehetővé tegyük, szükségünk van egy fájlra az XP-lemezről. Ennek kimásolásához szükségünk lesz az *ISOBuster* nevezetű programra **(www.smart-projects.net/isobuster/).** Töltsük le, majd telepítsük, végül indítsuk el az ISObustert.

Tipp
Az ISOBuster kezelőfelülete nyelvének a magyart is beállíthatjuk.

Amikor berakjuk az XP CD-t, válasszuk a bal oldalon található *Bootable CD* pontot. Ekkor a jobb oldalon feltűnik egy fájl a *Microsoft Corporation.img* névvel (vagy valamilyen más elnevezéssel – a lényeg, hogy *.img*



ISObuster: a bal oldali panelen válasszuk a Bootable CD pontot

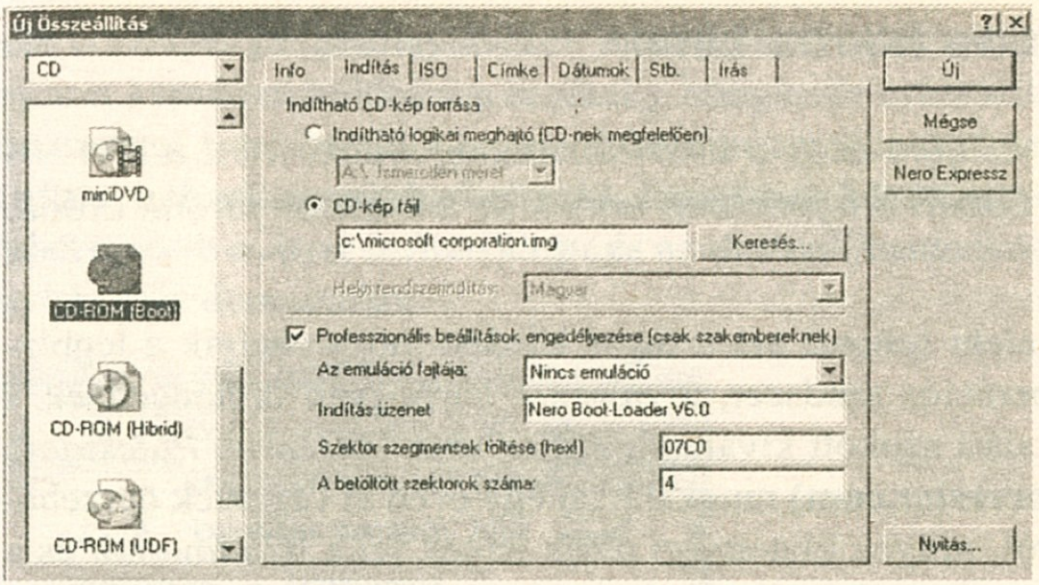
kiterjesztésű legyen). Ezt a piciny állományt kell kicsomagolnunk, méghozzá úgy, hogy a jobb gombbal rákattintanunk, majd a *kifejt • extract* parancsot választjuk. Ezt másoljuk a *c:* gyökérkönyvtárába, majd zárjuk be az ISObustert.

Ezután jegyezzük fel az XP CD-nk nevét – a *Sajátgépnél* vessünk rá egy pillantást. Ez lehet például *WXPOEM_HU*, de ettől eltérő is a különböző XP változatok esetében. Most már csak az a dolgunk, hogy XP CD helyett egy üres lemezt helyezzünk a CD-írónkba, és már kezdetét is veheti a következő lépés, a CD megírása.

5.5 A CD megírása

Az írás műveletét a *Neróval* mutatjuk be. Ennek két oka van: egyfelől a Nero az egyik legnépszerűbb írószoftver, másfelől segítségével megoldható a bootolható XP CD írása.

Indítsuk el a *Nero Burning ROM*-ot. Az *Új összeállítás* ablakban válasszuk a *CD-ROM (boot)* opciót. Az *Indítás* fülön, a CD-képfájlnál adjuk meg a *c:\microsoft corporation.img* fájlnevet (a *Keresés* gombbal hamar fellelhetjük). Ezután pipáljuk ki a *Professzionális beállítások engedélyezése* négyzetet, ami hozzáférést biztosít a további – szükséges – beállításokhoz. Az *Emuláció fajtájánál* adjuk meg a *Nincs emulációt,* majd változtassuk *A betöltött szektorok számát* 4-re. A *Szektorszegmensek töltését* feltétlenül hagyjuk a megadott 07C0 értéken.



Nero: az Indítás fülön eszközölt beállítások

Ha ezzel megvagyunk, kattintsunk a *Címke* fülre, ahol adjuk meg az XP CD-nk korábban feljegyzett nevét (a mi esetünkben ez a már említett WXPOEM_HU volt). Ha ez is megtörtént, nyomjunk az ablak jobb oldalán található *Új* gombra. Ekkor megjelenik a Nero Burning ROM fő ablaka.

Az ablak jobb oldalán keressünk rá a *c:\xp* mappára. Válasszuk ki az összes ott található fájlt, majd másoljuk az új CD-re. Ezután már csak annyi a feladatunk, hogy rábökjünk az írást aktivizáló gombra.

5.6 Az elkészített CD tesztelése

Miután elkészült a CD-nk, érdemes tesztelni egy olyan rendszeren, amelyen nyugodtan kísérletezhetünk (azaz nincsenek életbevágóan fontos adatok rajta), vagy egy *Microsoft Virtual PC*-vel vagy *VMWare*-rel létrehozott virtuális gépen. Az elkészült CD-nek akadálymentesen bootolnia kell. Emellett a telepítés után érdemes megbizonyosodnunk az integrálás sikeréről is, amit úgy tehetünk meg, hogy a *Start* menü *Futtatás* parancsmezőjébe begépeljük a *winver* parancsot, amely elénk tárja a gépen futó Windows verziószámát. Ebből hamar nyilvánvalóvá válik, hogy az SP2 telepítésre került-e. A munka végeztével persze ne feledkezzünk meg a c:\microsoft corporation.img állomány és a c:\xp, valamint a c:\sp2 mappák törléséről sem.

6 Windows kontra Linux

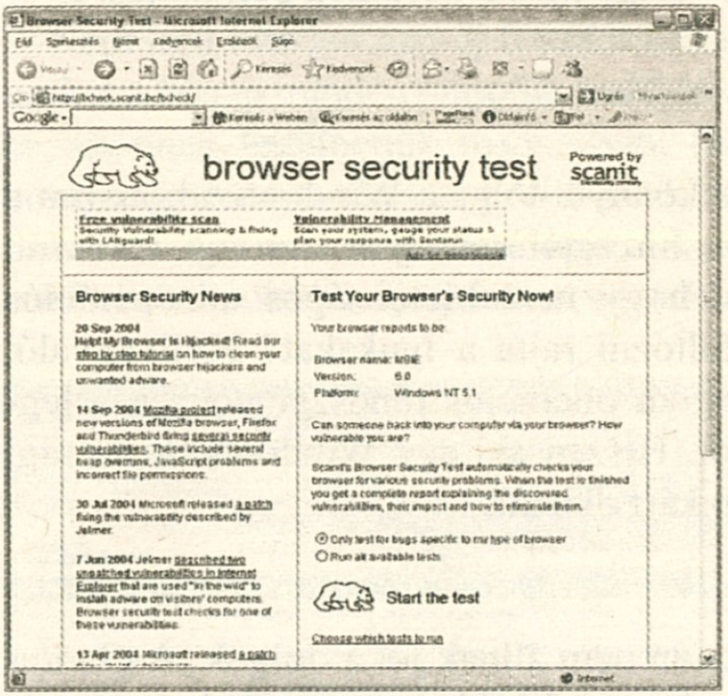
Sokan állítják, hogy a Linux biztonságosabb, mint a Windows. Ebben a fejezetben ennek az állításnak járunk utána.

Ahányszor valaki felteszi azt a fogas kérdést, hogy melyik a legbiztonságosabb operációs rendszer, a válasz – bárhogyan is hangozzék – heves felháborodást szokott kiváltani. A *Forrester Research Piackutató Intézet* **(www.forrester.com)** munkatársai egy éven át végeztek összehasonlításokat arról, milyen biztonsági rések léptek fel a *Windowsnál* és a különböző *Linux-disztribúcióknál,* és ezek mennyire voltak súlyosak. Az eredmény: a Forrester szerint egyedül a *Microsoft* tudott lezárni minden felmerült biztonsági rést – méghozzá a leggyorsabban. A különböző Linux-származékok, mint a *SuSE*, a *Red Hat,* a *Mandrake* és a *Debian* gyártói „csak" 99 százalékot értek el – hosszabb reakcióidőkkel. Alig jelent meg ez a tanulmány 2004 márciusában, máris záporozni kezdett a Linux-disztribútorok és -hívek kritikája, akik kétségbe vonták a Forrester-módszer gyakorlati hasznát. Hasonlítsuk most össze mi is a *Windows XP Professionalt* és a *SuSE Linux 9.1 Professional* verzióját.

A *CHIP* tesztlaborjában mindkét operációs rendszert háromfokozatú vizsgálatnak vetettük alá.

Az első fokozat a *biztonság az interneten:* először mindkét operációs rendszert „a dobozból kivéve", tehát *patchelés* nélkül telepítettük és vetettük alá a *Qualys* online biztonsági ellenőrzésének. Ez a keménységi próba az egész rendszert végigkopogtatja ismert biztonsági réseket – jelenleg több mint 3500-at – keresve, és ezeket öt veszélyességi osztályba sorolja. Minél magasabb a besorolási fokozat, annál súlyosabb a biztonsági hiányosság. Ezután telepítünk minden, a teszt időpontjában rendelkezésre álló szervizcsomagot, patchet és frissítést. Ha a tűzfal nincs automatikusan bekapcsolva, kézi vezérléssel aktiváljuk. Ezután mindkét operációs rendszert újból alávetettük a biztonságirés-vizsgálatnak. Ezen kívül mindkét operációs rendszerhez más böngésző járul, amelyeknek különböző az alapértelmezett konfigurációja, és más-más technikákat használnak. A Linuxé például egyáltalán nem ismeri az olyan potenciáli-

san veszélyes programnyelveket, mint az *ActiveX* és a *VBS*. Az internetre nyitott kapuként különösen érzékeny böngészőt ezért külön vetjük alá a biztonsági szakértők egy böngészőtesztjének, ez a *scanit* **(http://bcheck.scanit.be/bcheck).** Ez többek között azt ellenőrzi, hogy lehetséges-e a *Java,* a *JavaScript* és az *ActiveX* használata vagy az átirányítás más domainekre.



Indulhat a böngészőteszt!

A második fokozat *valamennyi lyuk bestoppolása kézzel:* amennyiben a patchek és frissítések ellenére még mindig maradtak biztonsági rések, akár a böngészőben, akár az operációs rendszerben, ezeket magunk foltozzuk be; ha lehetséges, a rendszer „saját fedélzeti eszközeivel". Ha ezek nem elegendőek, például a vírusvédelemnél, megnevezzük a felhasznált segédprogramokat.

A harmadik fokozat a *biztonság a számítógépen:* nem minden veszély érkezik az internetről. Előfordulhat az is, hogy a kém mellettünk ül az irodában. Ezért a két operációs rendszer biztonsági stratégiáit lokális szinten is nagyító alá vettük. Mennyire könnyű kijátszani a bejelentkezési jelszavakat, és mennyire jól vannak kódolva? A felhasználókezelésnek és a jogok kiosztásának is nagy szerepe van: milyen lehetőségei vannak a rendszergazdának például arra, hogy a merevlemez egyes terüle-

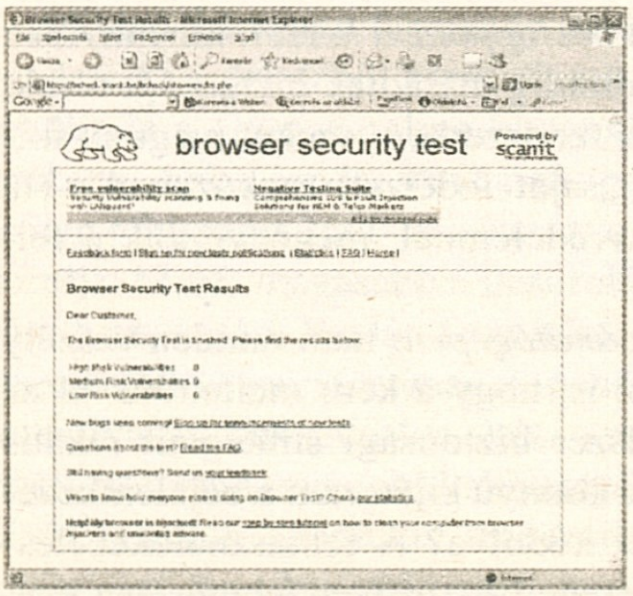
teit csak bizonyos felhasználócsoportok számára tegye elérhetővé? A felhasználóbarát backup-koncepciók is hozzájárulnak az adatbiztonsághoz. Három fokozatú ellenőrzőrendszerünk tehát ezeknek a szempontoknak az alapján tárja fel a két operációs rendszer erősségeit és gyengéit. Az alábbiakból egyébként az is kiderül, hogyan építhetjük erődítménnyé saját operációs rendszerüket. Terjedelmi okok miatt itt csak a Windows XP rendszeren végzett vizsgálataink kerülnek bemutatásra.

6.1 Windows XP

A Microsoftnak valóban nincs könnyű dolga a Windowszal, hiszen a weben naponta kapnak szárnyra híresztelések új biztonsági résekről. Van-e valami az előítéletekben, hogy nem biztonságos az operációs rendszer – és hogyan lehet befoltozni rajta a lyukakat? Nyilvánvaló, hogy a legszélesebb körben elterjedt operációs rendszer vonzza a legtöbb hackert és vírusprogramozót. Hiszen aki egy Windows biztonsági rést céloz meg, az tudja a legtöbb kárt okozni.

6.1.1 Biztonság az interneten

A Microsoftnál először egyáltalán nem állnak jól a dolgok. A *Qualys Check* több mint 25 biztonsági rést tár fel, lényegesen többet, mint a

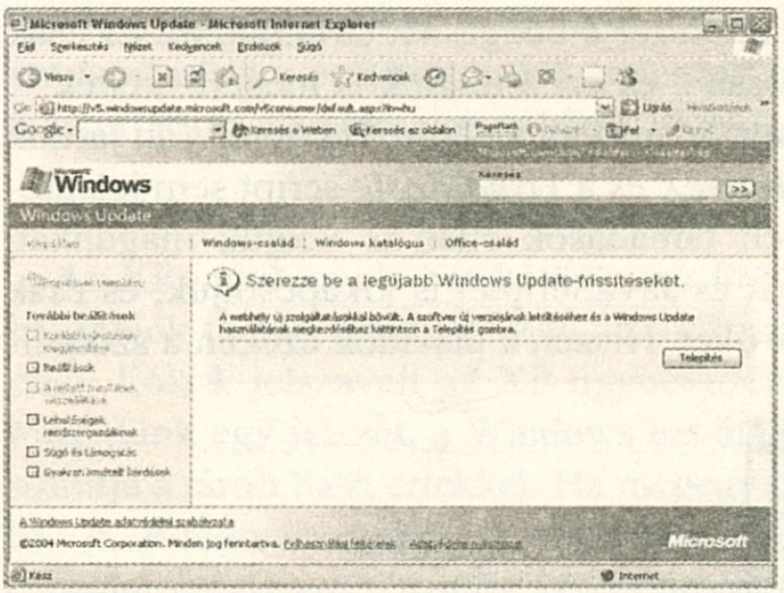


A 2. szervizcsomag telepítése meghozta a várt eredményt: a böngésző sebezhetőségei egytől egyig eltűntek

SuSE Linuxnál, ráadásul ebből ötöt a legmagasabb veszélyességi fokozatban. A Microsoft azonban a 2. szervizcsomaggal és az aktuális patchekkel gondoskodik a segítségről. Ezek telepítése után a Windows XP-nek már nincs mit a szemére vetni. Tehát az XP-vel a legfrissebb update nélkül ne merészkedjünk a webre!

6.1.2 Biztonsági frissítések telepítése

Nem kell minden nap új frissítéseket keresgélnünk, mert a redmondiak ezeket a hónap minden második keddjén összegyűjtve felteszik az internetre, ahonnan letölthetjük manuálisan, **(http://windowsupdate.microsoft.com)** vagy automatikusan, a Windows XP-be integrált update-modul használatával. Ezt az automatikát úgy is konfigurálhatjuk, hogy az operációs rendszerünk minden új update-et és patchet maga töltsön le és telepítsen.



A Windows Update oldairól letölthetjük a legfrissebb javításokat

6.1.3 Bekapcsolt tűzfal

Csak a 2. szervizcsomaggal kapunk automatikusan bekapcsolt tűzfalat, amely véd minden fontos hálózati és telefonos kapcsolatot. A rendszer minden ICMP-csomagot, mint például a Ping parancsot, kompletten blokkol. Így csaknem láthatatlanul internetezhetünk: az XP számítógépünk lehetséges támadóinak minden kérését a nagy semmibe irányítja. Ehhez nincs is szükség további beállításokra, minden optimálisan konfi-

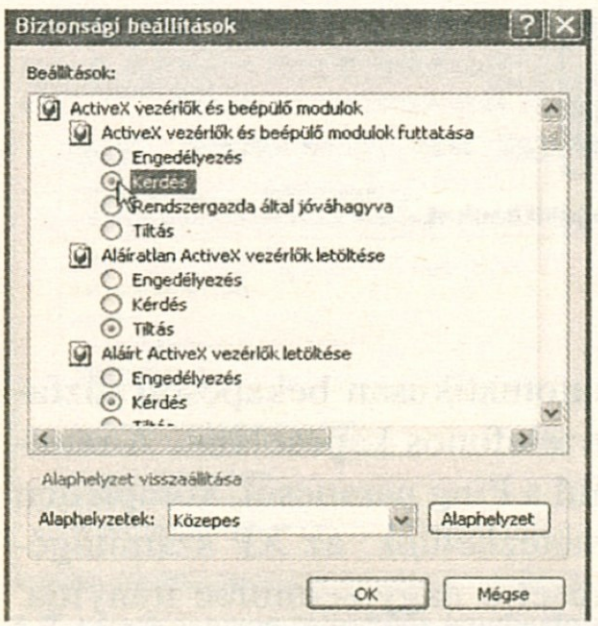
gurált. És ha egyik vagy másik programnak mégis szüksége van egy portra, a Windows automatikusan rákérdez, hogy megnyithatja-e.

6.1.4 Külön vírusvédelem telepítése

A vírusírók kinézték maguknak a Windowst: az antivírusgyártó *Sophos* szerint 2003-ban több vírus és féreg volt, mint előtte valaha – és a tendencia növekvő. Mivel a legtöbb vírusíró célja, hogy minél több számítógépet fertőzzön meg, a Windows 90 százalékos részesedésével az otthoni számítógépek piacán igencsak alkalmasnak tűnik erre a célra. Az ilyen veszélyek ellen a Windows XP önmagában nem nyújt védelmet. Ezeket a feladatokat kiegészítő programoknak, esetünkben a vírusvizsgálóknak kell átvenniük, mint amilyen például a *Norton Antivirus* és társai.

6.1.5 A böngésző biztonságossá tétele

A Windows XP az *Internet Explorer 6* böngészőt tartalmazza. Ez csak úgy tehető teljesen biztonságossá – és ezt a tesztek is megerősítették –, ha minden frissítést akkurátusan telepítünk a gépre. Ha gondosan járunk el, a két problémás elem, az *ActiveX* és a *VisualBasic* script sem jelentenek veszélyt. Hogy a jövőbeli támadások ellen is védjük magunkat, jobb, ha az ActiveX-et, a Javát és JavaScriptet is kikapcsoljuk, és csak szükség esetén engedélyezzük őket. Hiszen a támadók ezeken a szolgál-



Ha bejelöljük a Kérdés opciót, a Windows minden ActiveX elem futtatása előtt engedélyt kér

tatásokon keresztül tudják a legtöbb kárt okozni. Ehhez nyissuk meg az Internet Explorert, és kattintsunk az *Eszközök* menüben az *Internetbeállításokra.* A következő ablakban válasszuk a *Biztonság* fület, és kattintsunk az *Egyéni szint...* gombra. Most az *ActiveX vezérlők és beépülő elemek futtatása* előtt kapcsoljuk be a *Kérdés* opciót.

A Windows XP most minden ActiveX elemnél meg fogja kérdezni, hogy az Internet Explorer futtassa-e. Ugyanez érvényes a Javára is: állítsuk ugyanebben az ablakban a Java engedélyeket *Magas biztonságra.*

6.1.6 Biztonság a számítógépen

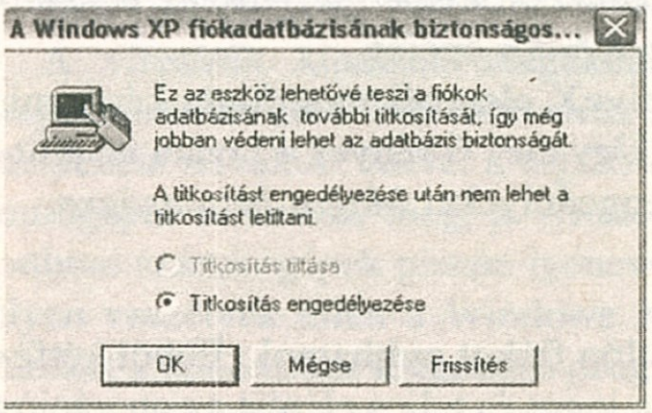
XP alatt minden felhasználónak külön fiókot nyithatunk. Ebből kétféle van: az egyiknél megadunk minden jogot és teljes elérést az operációs rendszer minden funkciójához, a másiknál korlátozzuk a jogokat. A második kategóriába tartozó felhasználóknak ugyan elérésük van a rendszerhez, de nem tudnak szoftvereket telepíteni vagy rendszerbeállításokat módosítani. A felhasználókezelésnek és a jelszavas hozzáférésnek a gyakorlatban azonban van néhány hiányossága.

6.1.7 Felhasználói fiókok biztonsága

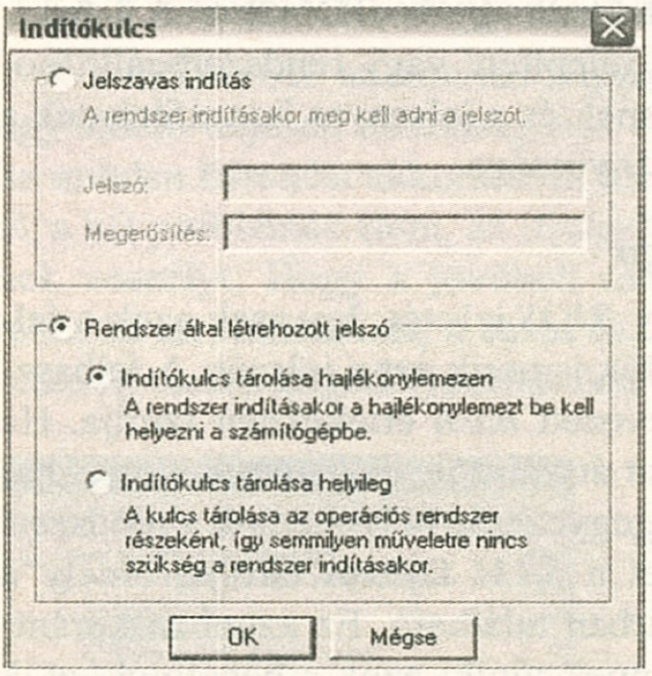
Az XP indulása elé betehetünk egy *BIOS* jelszót. Így csak azok a felhasználók tudják elindítani a PC-t, akik ismerik ezt a jelszót. A felhasználói fiókok jelszavait az XP úgynevezett *hash* értékekben tárolja. Ha megadunk egy jelszót, a Windows ezt átszámítja, és az értéket összehasonlítja a tárolt hash értékkel. Ha megegyeznek, beléphetünk a rendszerbe. A Windows ezeket az értékeket a *SAM* fájlban tárolja, amely a *c:\windows\system32\config* könyvtárban található. Ez azonban korántsem olyan biztonságos, mint amilyennek tűnik: azok a behatolók, akik elérik a helyi rendszert, néhány egyszerű, internetről letölthető segédprogrammal a tárolt hash értéket átírhatják a saját értékükre. Így elérést nyernek a rendszerhez. Ez ellen a nagyon biztonságosnak számító *EFS (Encrypting File System)* jelent segítséget, amellyel titkosíthatjuk a fájlrendszert, hogy csak az arra jogosult felhasználók láthassák a merevlemez tartalmát.

Ehhez indítsuk el a *Start\Futtatás\syskey* programot, és nyomjuk le az *Entert.* A következő ablakban menjünk a *Frissítésre.* Ezután több beállí-

tási lehetőséget látunk. A legbiztosabb megoldás: generáltassunk jelszót a rendszerrel, és végül mentsük flopira, amelyet minden rendszerindításkor be kell helyezni.



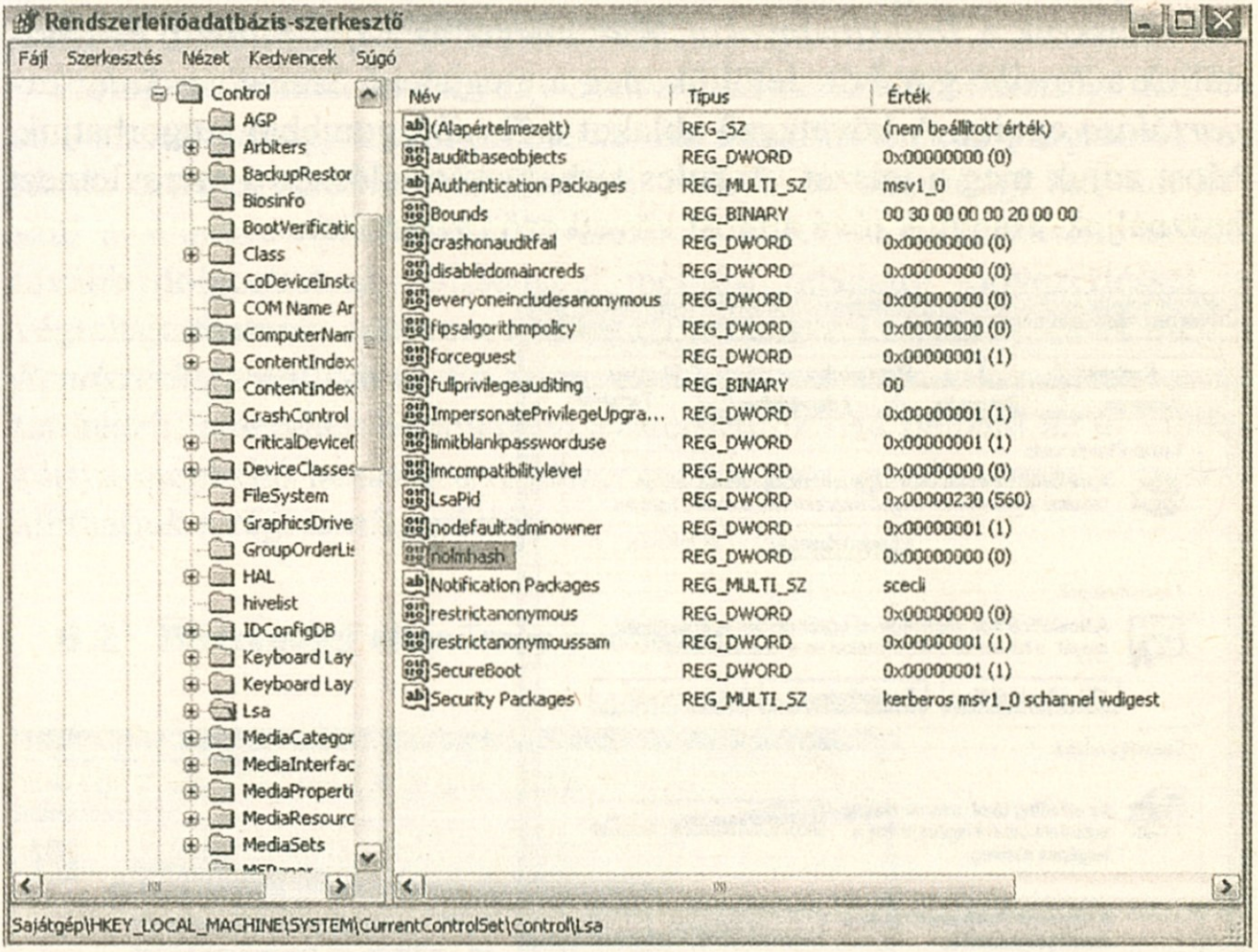
A syskey programmal az XP fiókadatbázisát titkosíthatjuk



A rendszer által generált jelszót flopin is tárolhatjuk

A felhasználókezelésnél van még egy biztonsági rés. Ha egy felhasználó megváltoztatja a jelszavát, a Windows ezt két hash értékben tárolja, és mindkettő bekerül a SAM fájlba. A második érték neve *LMHash (LAN Manager Hash):* ez egy relikvia a Windows 3.1-es időkből, és csak kompatibilitási okokból készül. A hackerek dolgát az LMHash nagyon megkönnyíti, mert csak nagybetűket ismer, és ezzel a lehetséges jelszókombinációk száma jelentősen csökken. Ezért ha csak XP-t hasz-

nálunk, kapcsoljuk ki a második hash értéket. Ehhez kattintsunk a *Start* menüben a *Futtatásra,* írjuk be: *regedit,* és kattintsunk az *OK*-ra. Ezután menjünk a *HKEY_LOCAL_MACHINE SYSTEM/CurrentControlSet/Control/Lsa* kulcsra. A jobb oldalon kattintsunk duplán a *nolmhashre*, és az *Érték* alatt adjunk meg 1-et. Egy kattintás után az *OK*-ra zárjuk be a Registry-szerkesztőt, és indítsuk újra a PC-t.



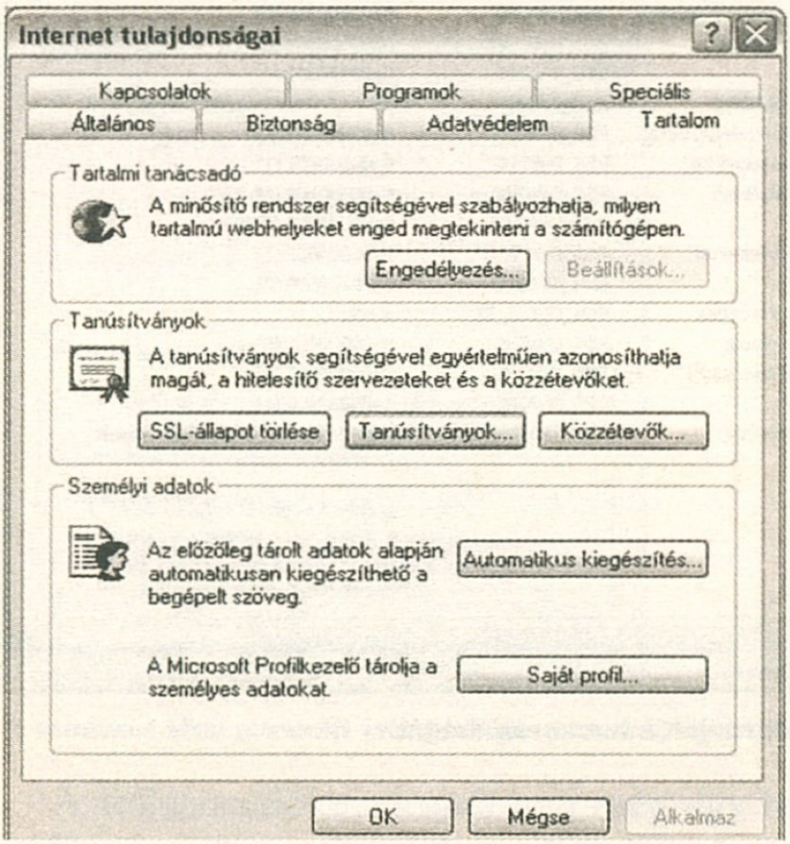
A Registry módosításával tovább nehezíthetjük a hackerek dolgát

6.1.8 Mappák kódolása

Ha *XP Professionalt* használunk, az *NTFS* mappákat titkosíthatjuk. Ehhez kattintsunk a jobb egérgombbal a mappára, és válasszuk a *Tulajdonságokat.* A *Speciális* alatt menjünk a *Tartalom titkosítása...* menüpontra. A fájlok mostantól kezdve 4096 bites kóddal védettek – egy hackerélet nem lenne elég a feltöréséhez. Ez a fajta titkosítás nem jel-

szót, hanem egy rendkívül biztonságos tanúsítványt használ, amelyet a számítógépre kell telepíteni, és egyfajta kulcsként szolgál. A hacker csak ezzel tudja elérni az adatokat. Ezért exportáljuk a tanúsítványt, és utána töröljük a merevlemezről. A kódolt adatok csak így lesznek valódi biztonságban.

Ez így történik: *Kattintsunk* a *Start* menüben a *Beállításokra,* utána a *Vezérlőpultra* és végül duplán az *Internetbeállításokra.* A *Tartalom* fülnél válasszuk a *Tanúsítványokat.* Kattintsunk az *Exportálásra,* és használjuk a *Tovább* gombot. Jelöljük meg a megjelenő *Személyes kulcs exportálása* opciót. A következő ablakot a *Tovább* gombbal átugorhatjuk. Most adjuk meg a jelszót. A kulcs tárhelyeként először a merevlemezt használjuk. Hagyjuk jóvá a most következő üzeneteket.



A fontos állományainkat tanúsítványokkal is védhetjük

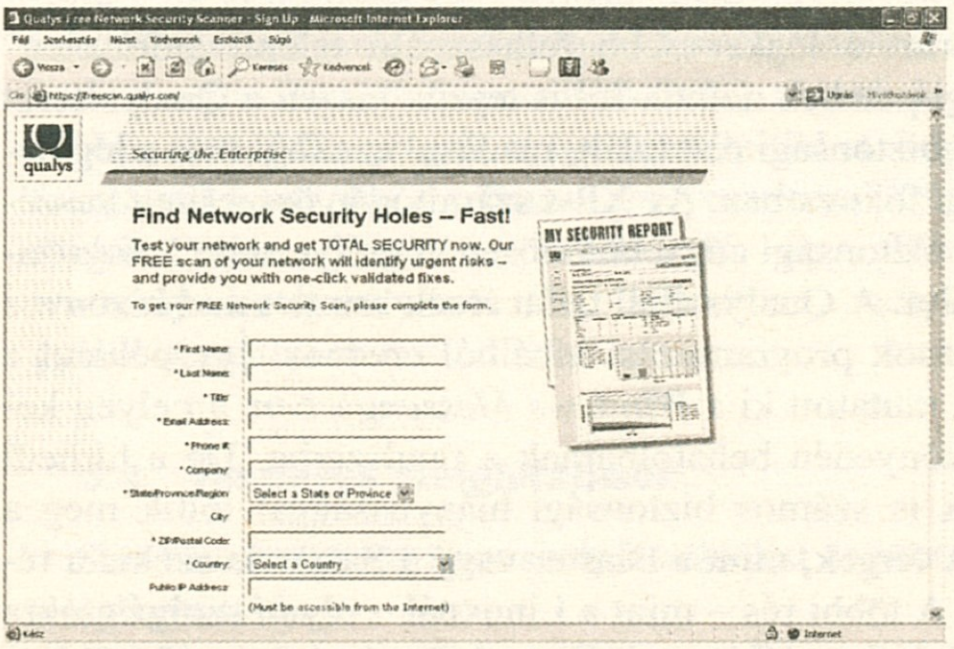
Most a *Tanúsítványok áttekintéséhez* jutottunk. Válasszuk az *Eltávolítást,* és a biztonsági kérdésre válaszoljunk igennel. Helyezzük át az exportált kulcsot a merevlemezről egy külső tármédiumra, például flopira vagy memóriakártyára. A fájlról készítsünk másolatot, mert ha elveszít-

jük a kulcsot, semmilyen lehetőségünk nem marad, hogy az adatokat elérjük. Mikor az adatokhoz akarunk jutni, importáljuk a kulcsot az adathordozóról dupla kattintással. Ez ugyan körülményes, de biztonságos. Ne felejtsük el a tanúsítványt minden Windows-leállítás előtt újból törölni a merevlemezről, mert a Windows a hozzáférési kulcsot minden alkalommal újból a merevlemezre menti.

6.1.9 Automatikus biztonsági mentés

Komplett adathordozók vagy csak a rendszerfájlok biztonsági mentése – az XP-vel egyik sem probléma. Az integrált backup programot varázsló teszi egyszerűen kezelhetővé. Miközben biztonsági másolat készül a Windows-partícióinkról, érezhető teljesítménykorlátozás nélkül tovább dolgozhatunk. Biztonsági mentési feladatot idővezérléssel is végrehajtathatunk. Aki nem akar igazi backupot készíteni, annak elég a *Rendszerhelyreállítás* is. Ez az egyes telepítések után visszaállítási pontot készít, amelyhez bármikor visszatérhetünk. Ha például az új videokártya-meghajtó bezavar a rendszer indításakor, gombnyomásra visszaállíthatjuk a régi konfigurációt.

6.2 Biztonsági ellenőrzés profiktól



Ingyenesen tesztelhetjük hálózatunkat biztonsági szempontból a Qualys oldalán

A CHIP a rendszerek biztonságát a *Qualys* amerikai vállalat szakembereivel együttműködve tesztelte. A Qualys a világszerte vezetőnek számító biztonsági cégek egyike, és negyedévenként körülbelül egymillió biztonsági elemzést végez. Referenciahelyei közé tartozik többek között az USA kormányzata is. Magánszemélyeknek a Qualys ingyenes ellenőrzést kínál **(https://freescan.qualys.com/),** amely a tíz legsúlyosabb biztonsági résre vonatkozik.

A profi ellenőrzések csak vállalatoknak készülnek, és az áruk ötjegyű számmal írható le (dollárban számolva). Az általunk használt *Enterprise* verzióban a Qualys fejlesztette tesztprogram 3500 jelenleg ismert és súlyos biztonsági rést keresve ellenőrzi a számítógépet. A teszt nagyon nagy pontossággal működik, a hibaszázalék 0,003 százaléknál alacsonyabb. A biztonsági ellenőrzés a számítógép minden lényeges biztonsági jellemzőjét teszteli az internet- és az online biztonság területén. A sebezhetőségi pontokat a Qualys öt különböző fokozatba osztja be: az első fokozat csekély veszélyt jelent, az ötödik fokozat súlyos biztonsági rést jelöl a rendszeren.

6.3 Teszteredmények

6.3.1 Windows XP Professional

A Microsoft szerint a legkevesebb felhasználó telepít „meztelen" Windowst biztonsági patchek nélkül. Jól is teszik, hiszen a Qualys-teszt – írd és mondd – 25 biztonsági rést talált, ráadásul ezekből ötöt a legmagasabb veszélyességi fokozatban. Az XP-s számítógép összesített veszélyességi fokozatát a biztonsági cég a különösen veszélyeztett (5. fokozatú) kategóriába sorolta. A Qualys által talált rések szinte mind bizonyos Windows-szolgáltatások programozási hibáiból erednek. Így például a teszt biztonsági rést mutatott ki a *Windows Messengerben,* amelyen keresztül a támadók könyedén behatolhatnak a rendszerbe. De a hírhedt puffertúlcsordulások is számos biztonsági hiányossággal töltik meg a tesztek hibalistáit. A férgek, mint a Blaster vagy a Sasser is ezeket a réseket használják ki. A többi rés – mint a Linuxnál – olyan szolgálatokra vonatkozik, amelyek információt szolgáltatnak a számítógépről, például

az *ICMP (Internet Control Message Protocol),* amelyen keresztül a támadó többek között megtudhatja, melyik szolgáltatót használjuk. Ilyen sok potenciális támadási pont láttán nagy volt a meglepetés a frissítések és a 2. szervizcsomag telepítése után: ezek minden rést lezártak, s a számítógépről semmilyen információ nem maradt kívülről látható – nagy piros pont a Microsoftnak.

6.3.2 SuSE Linux 9.1 Professional

Az általános vélekedés, miszerint a Linux bombabiztos, a SuSE standard installációjában nem állja meg a helyét: a Qualys 15 rést talált, ezek azonban messze nem olyan kockázatosak, mint a Windowséi. Egy támadás összkockázatát a Qualys középerősségűnek, 3. fokozatúnak sorolja be. A lékek szinte kizárólag csak kifelé látható szolgáltatásokra vonatkoznak. Támadási pontként csak akkor jönnek számításba, ha ezekben a szervizekben hibák kerülnek felszínre. Az egyetlen 3-as fokozatú rés a *Secure Shellt (SSH*-t) érinti, amely a biztonságos kapcsolatról gondoskodik. Ez az *OpenSSH* verzió tartalmaz egy bugot, amely a támadóknak puffertúlcsordulás révén hozzáférést engedélyez a rendszerhez.

Két további rés (2. fokozat) az *RPC* szolgáltatásra és az *ICMP* üzenetekre vonatkozik. Kifelé egy portmapper látszik, amely RPC-kéréseket továbbít a rendszerszolgálatoknak. Ha egy betolakodónak sikerül kikerülnie, és elindítania egy szolgáltatást, egy privilegizált portról kaphat hozzáférést a Linux-rendszerhez. Ezen az online update sem változtat, csak a manuálisan bekapcsolt tűzfallal zárunk le 10 rést. A SuSE továbbra is reagál a pingekre: így tesztelni lehet, hogy egy számítógép elérhető-e. Ugyanakkor a *Traceroute* paranccsal követni lehet az adatcsomagok útját. Végül a betolakodó egy *Whois* lekérdezéssel a **www.ripe.net/perl/whois** alatt kideríthetí, melyik szolgáltatóhoz vagyunk becsatlakozva.

6.4 Veszélyes szolgáltatások

Sok biztonsági rés érint szolgáltatásokat és protokollokat. Ezek közül a legfontosabbak:

ICMP: az *Internet Control Message Protocol* hibajelzéseket szállít az

IP, UDP és *TCP* hálózati protokolloknak. A legismertebb ICMP üzenet a *ping* parancs. Az ICMP üzenetek sokfélesége (kb. 20) lehetővé teszi a betolakodónak, hogy információkat gyűjtsön egy rendszerről úgy, hogy megfelelő ICMP csomagokat küld.

RPC: a *Remote Procedure Call Protocol* funkciókat indít el más számítógépeken, például a *Remote Computingnál.*

UDP: a *Users Datagram Protocol* – mint a TCP –, egy kommunikációs protokoll a számítógépek között, és szintén az *Internet Protocolon (IP*-n) keresztül kommunikál.

TCP/IP: az *Internet Protocol (IP)* részekre bontja és címezi, majd továbbítja az adatokat. A *Transmission Control Protocol (TCP)* ráépül, gondoskodik a csomagok helyes sorrendjéről, és zavarmentes kommunikációt biztosít.

7 12 kérdés a 2. szervizcsomagról

A Microsoft most minden idők „legméretesebb" Windows-frissítését kínálja. Valóban megéri-e telepíteni ezt az óriáscsomagot? Ebben a fejezetben a 12 legégetőbb kérdésre keressük a választ a szervizcsomaggal kapcsolatban.

A sanyarú sorsú Windows XP felhasználóknak az utóbbi időben igen gyakran kellett új biztonsági rések ellen küzdeniük. Be tudja-e végre váltani a 2. szervizcsomag a biztonságra vonatkozó ígéreteket? Milyen titkos képességeket kínál a felhasználóknak? Hagyja-e majd akadálytalanul működni a vírusvizsgálókat? Rögtön kiderül.

7.1 Melyik vírusvizsgáló kompatibilis az SP2-vel?

A szervizcsomagban minden az új *Biztonsági központ* körül forog, amelyet a *Vezérlőpult/Biztonsági központ* alatt találunk. Itt három biztonsági összetevőről kapunk áttekintést: a tűzfalról, a frissítésekről és a

vírusvizsgálóról. A vírusvizsgálók azonban nem a Microsofttól jönnek. Ahhoz, hogy a Biztonsági központ felismerje az antivírus programokat, azokat egy meghatározott portra kell beállítani. Béta-stádiumban ez a lehető legkevesebb vírusvizsgálóval sikerülhet – a *Vírusvédelem* menüpont pirossal kijelölve és veszélyként besorolva maradt. Nézzük, mely vírusvizsgálók működnek együtt az SP2-vel.

Kaspersky Antivirus: a *v5.0.124* verziótól idomul a Biztonsági központhoz. A frissítést ingyen adják.

Sophos Antivirus: A legújabb verzió szeptembertől már boldogul az SP2-vel.

Norton Antivirus: a *Symantec* a *Live Update-tel* teszi SP2-kompatibilissé a termékét.

Trend Micro: az SP2 felismeri a Trend Micro *PC-Cillin Internet Security (TIS) 11.x*-et és a korábbi verziókat, sőt az *OfficeScan Corporate Edition 5.5x*-et és *6.5*-öt is.

McAfee: az SP2 *6.0*-tól *9.0*-ig a *McAfee VirusScan* minden verzióját felismeri.

BitDefender: a szoftver a *Live Update*-en keresztül SP2 kompatibilissé avanzsál.

AntiVir: A támogatás már integrálva van, és a *6.26*-os verziótól rendelkezésre is áll. A régebbi verziók nem támogatják a Biztonsági központot.

Panda Antivirus: Minden verzió kompatibilis. A felhasználók automatikus update-et kapnak.

VirusBuster: Valamennyi termékbe beépítették már az új Windows Biztonsági központ támogatását, így a termékek frissítései, illetve a védelem állapota a Windows saját felületéről is ellenőrizhető.

7.2 Milyen előnyei vannak az új tűzfalnak?

Először is: egy *Blastert* az új tűzfallal már nem kapunk el olyan könnyen, ugyanis a védelem már az első bootolásnál aktív. A tűzfal ilyenkor alapvetően mindent blokkol, csak speciális információkat, például a domain-szerverről, engedélyez. A szolgáltatás, amely további kivételeket enged meg, csak később indul el. Ezen kívül az új *Windows Firewall*

megérteti magát a következő internetszabvánnyal, a 6-os verziójú *Internet Protokollal (IPv6)* is. Ez a jövőbeni újítás az IP címeket 128 bitre bontja fel, és így több hosztot tesz lehetővé az interneten. A tűzfal ennél is ugyanazt a kivétellistát használja, mint az IPv4-hez.

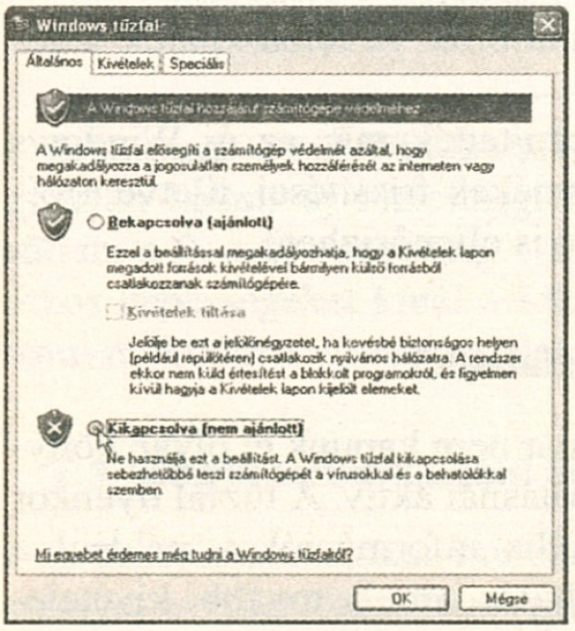
7.3 Mikor kapcsoljuk be a tűzfalat, és mikor ne?

Mikor éri meg használni a tűzfalat? Válasz: kétség esetén mindig. Néhány példa és ajánlás:

ISDN/ADSL: számítógépünkkel közvetlenül csatlakozunk egy ISDN vagy ADSL vezetékre. Tehát mondhatni védtelenek vagyunk. Ajánlás: feltétlenül működtessük a tűzfalat!

Router: routeren keresztül jutunk az internetre. Az ilyen eszközöknek többnyire saját tűzfaluk van. Attól függően, hogy mennyire bízunk meg ennek a konfigurációjában, lemondhatunk az XP tűzfalról. Ártani mindenesetre nem árt. Ajánlás: aki nem teljesen biztos a dolgában, jobb, ha bekapcsolva hagyja.

Hálózatban: itt érdemes minden PC-t XP tűzfallal védeni, akkor semmiképpen sem jutnak be a Blasterek, Sasserek és társaik az internetről. Notebook dockinggal a károkozók éppúgy bejuthatnak a hálózatra, hogy azután belülről eluralják. Ajánlás: hagyjuk bekapcsolva.



Külső tűzfal használata esetén érdemes kikapcsolnunk a Windows tűzfalát

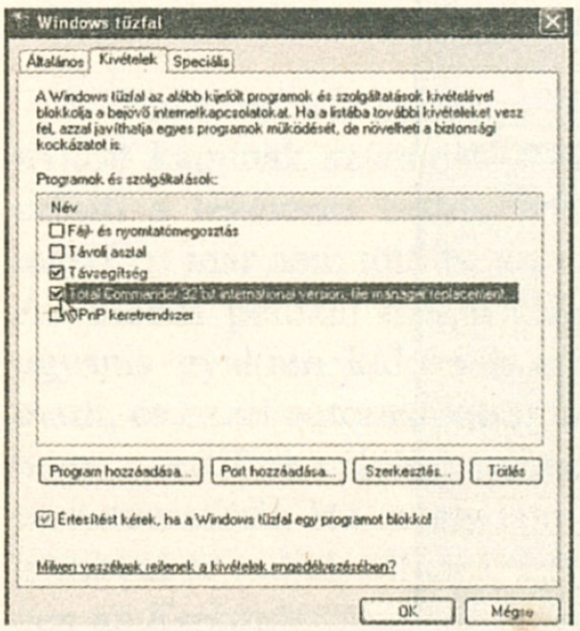
Desktop-tűzfal: eddig *ZoneAlarmot* vagy *Outpostot* használt, és szeretne megszokott szoftverénél maradni? A Microsoft szerint mindkét tűzfal működhet egymás mellett, de ennek nincs sok értelme. Aki egy másik tűzfalat szeretne használni, a Windowsét inkább kapcsolja ki: kattintson a *Vezérlőpulton* duplán a *Windows Tűzfal* ikonra és válassza a *Kikapcsolva* beállítást.

7.4 Hogyan konfigurálhatom a tűzfalat a legegyszerűbben?

A tűzfal praktikus módon szinte önmagát konfigurálja: ha egy program ki akar menni az internetre, megjelenik egy üzenetben, hogy melyik alkalmazásról van szó. Ilyenkor eldönthetjük, hogy az internetelérését minden esetben engedélyezzük-e, csak ez alkalommal hagyjuk jóvá, vagy általánosan blokkoljuk. Az alkalmazás mindenesetre felkerül a tűzfal listájára, amelyen később módosíthatunk.

7.5 Hogyan vonom meg a programoktól a kiadott engedélyt?

Ha meg akarjuk tagadni egy programtól a korábban kiadott elérési engedélyt, kattintsunk a *Vezérlőpulton* duplán a *Windows Tűzfal* ikonra, és válasszuk a *Kivételek* fület. A *Programok és szolgáltatások* mezőben

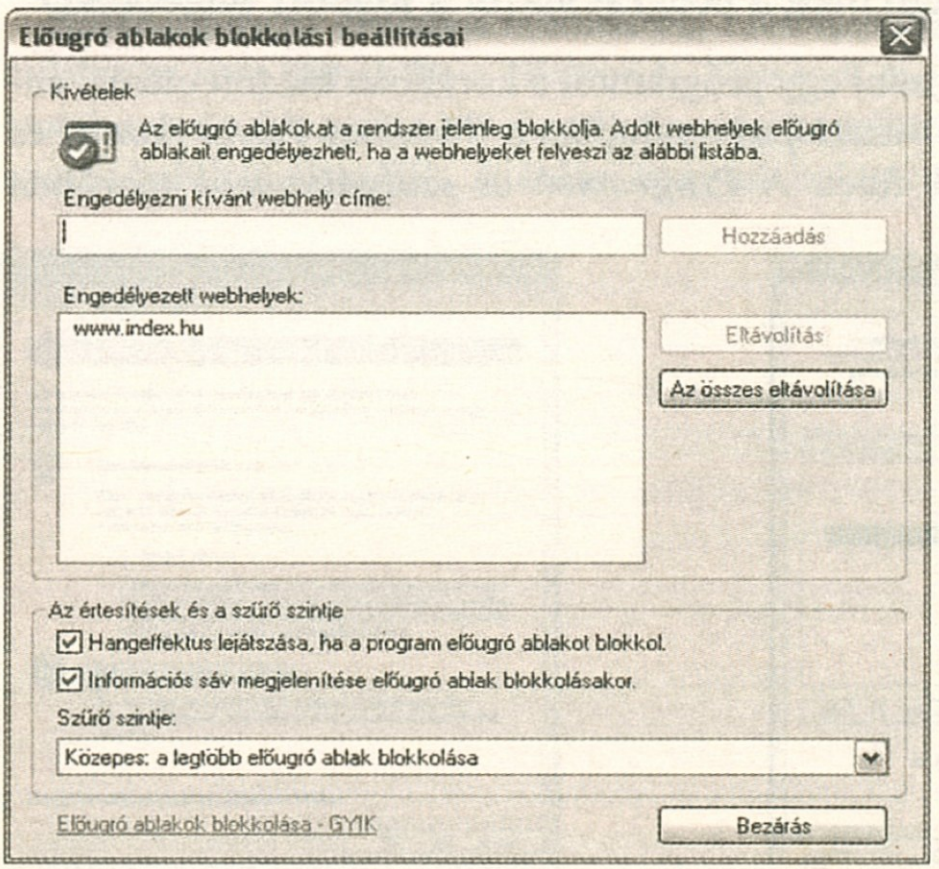


A Kivételek fülön megkurtíthatjuk a programok kijutásának szabadságát

most minden alkalmazást láthatunk, amelyeket a Tűzfal regisztrált. Itt egyszerűen elvesszük a pipát a program elől, amelyet zárolni akarunk.

7.6 Hogyan állítom be helyesen az Előugróablak-blokkolót?

A zavaró reklámokat, amelyek hirtelen saját ablakban jelennek meg, az SP2 *Előugróablak-blokkolója* automatikusan gátolja. A finomhangolásnak azonban itt is van értelme. A beállításokat az Internet Explorerben az *Eszközök/Előugró ablakok blokkolása/Előugró ablakok blokkolási beállításain* keresztül érjük el. A blokkoló szűrőfokozata kezdetben *Közepesen* áll – ez a legtöbb reklámbannert visszatartja. Akkor azonban nem, ha egy popup egy link mögött rejtőzik. Ha biztosra akarunk menni, állítsuk a szűrési fokozatot *Magasra.* A trükk: ha tudjuk, hogy egy link mögött előugró ablak rejtőzik, például, mert egy fórumról van szó, kikerülhetjük a védelmet a **Ctrl** gombot az egérkattintással együtt lenyomva. Ha ez tartósan túl körülményesnek tűnik, vegyük fel



A kivételek listáján szereplő weboldalak előugró ablakait nem zárja be az Internet Explorer

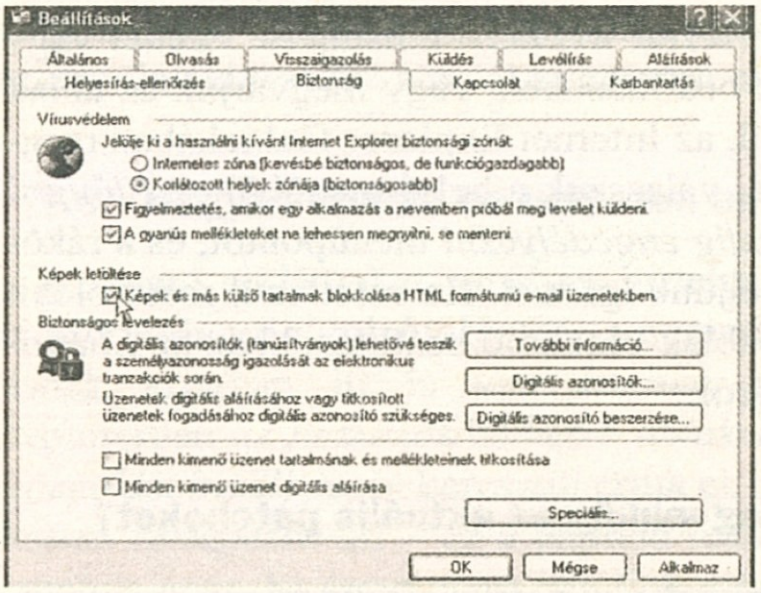
az érintett oldalakat az *Engedélyezett webhelyek* listájára. Ezeket vagy kézzel beírjuk az Előugróablak-beállításokba, vagy megvárjuk az ablak blokkolását. Ekkor ugyanis felül, az Internet Explorer főablakában megjelenik egy lista. Kattintsunk rá, válasszuk a helyi menüből az *Előugró ablakokat erről az oldalról mindig engedélyezni* menüpontot, és a rákövetkező biztonsági kérdésre feleljünk igennel. Ha véletlenül rossz oldalt engedélyeztünk, azt az Előugróablak-blokkoló beállításokban az *Eltávolítás* gombbal törölhetjük a listáról.

7.7 Hogyan kaphatom meg mindig az aktuális patcheket?

A Microsoft hangsúlyozza a biztonsági patchek fontosságát – ennyi javításnál ez nem is csoda. Hogy a telepítésük még könnyebben menjen, a fejlesztők felvették az automatikus update-et a Biztonsági központba. Alapértelmezésben a beállítása *Automatikus (ajánlott)*. De ha azt érezzük, hogy a Windows így túl gyakran avatkozik az életünkbe, kattintsunk lent a Biztonsági központban az *Automatikus frissítések* ikonra. A megjelenő ablakban előírhatjuk a Windows viselkedését. A legkevésbé idegesítő a *Csak értesítést kérek, de ne legyen automatikus a letöltés és a telepítés* beállítás. Teljesen azonban nem célszerű kikapcsolni az update-et.

7.8 A szervizcsomag most már az e-mailjeimet is védi?

A Windowsba beépített mail-kliens eddig a vírusok és trójaik számára nyitott kapunak számított. A 2. szervizcsomag két pontban legalábbis erősíti a levelezés biztonságát: egyrészt több fájlmellékletet blokkol, másrészt már nem tölti be automatikusan a képeket a HTML mailekben. Az utóbbi például megakadályozza a spamküldők kémkedését. Ezek ugyanis gyakran küldenek egy 1×1 pixeles képet. Ha megnyitjuk a mailt, és ezzel automatikusan betöltődik a kép, ebből a feladó megtudja, hogy a mailfiók valóban használatban van. Az SP2 megakadályozza ezt az automatikát. Ha mégis látni akarjuk a képet, egy újonnan megjelenő gombbal le tudjuk töltetni. Ezt a funkciót azonban az *Outlook Expressben* az *Eszközök/Beállítások/Biztonság* fülnél a *Képek és más külső tartalmak blokkolása* opciónál ki is kapcsolhatjuk.



A Képek és más külső tartalmak blokkolása új biztonsági funkció az Outlook Expressben

7.9 Milyen újítások vannak, amelyeket nem látunk azonnal?

A szervizcsomagnak köszönhetően további segédprogramok is felkerülnek a gépünkre:

MovieMaker 2.1: a videóvágó program aktuális verziója ugyan nem tartalmaz újabb funkciókat, de kiküszöböl néhány kisebb programhibát.

DirectX 9.0c: az új DirectX verzió.

Windows Media Player: a csomag tartalmazza a *Media Player 9.0*-s verzióját. A *Media Player 10* megjelenése is esedékes.

TabletPC bővítmények: többek között kapunk egy javított kézírásfelismerőt.

Windows Messenger: a Messenger-kliensnek most *4.7.3000* a verziószáma. A szoftver blokkolja azokat a fájlokat, amelyeknek a feladója nincs a kapcsolatok listán és a fájl megbízhatatlannak van besorolva, például mert futtatható.

Update-kezelés: a *Vezérlőpult* szoftverkezelője most már a telepített programok frissítéseit is regisztrálja.

Support segédprogramok: a rendszergazdáknak a Microsoft még update-eket is ad a support eszközökhöz. A legérdekesebb közülük talán az *Extract* parancs, amellyel CAB fájlok tartalmát lehet kicsomagolni. A segédprogramokat az SP2 CD-n a *Support Tools* mappában találjuk.

Windows Update: ha a felhasználó a *Start* menüben a *Windows Update*-re kattint, az új update oldalra jut.

7.10 Mindig újra kell telepítenem az SP2-t?

A Windows NT-nél és 2000-nél mondhatni kötelező volt minden hardvertelepítés után újból feltenni a szervizcsomagot. Így kellett felülírni a régi illesztőprogramokat, amelyek például az eredeti Windows CD-ről származtak, vagy amelyeket a hardverhez kaptunk. A 2. szervizcsomagnál ez okosabban van megoldva. Egy példa: a Windows XP sok meghajtót tárol a merevlemezen a *Driver.cab* fájlban. Ahelyett, hogy ezt felülírná, az SP2 létrehoz egy *sp2.cab* fájlt, amely az új meghajtókat tartalmazza. Hogy a Windowsnak melyik CAB-fájlban kell egy illesztőprogramot keresnie, az a *Drvindex.inf* fájlba van beírva. A szétválasztás révén tehát az eredeti és az SP2 már alig tesznek egymásnak keresztbe. Ebből következően az újratelepítgetés is a múlté.

7.11 Feltehetem az SP2-t és a Windowst egy CD-re?

Igen, méghozzá úgy, hogy az SP2 telepítésekor automatikusan felkerül a lemezre. Erről bővebben az 5. fejezetben olvashatnak.

7.12 A 2. szervizcsomaggal most teljes biztonságban vagyok?

Százszázalékos biztonság PC-n valószínűleg soha nem fog létezni. Az SP2 ugyan jóval hatásosabban felfegyverez a kívülről jövő veszélyek ellen, de azért még így is lehetnek gondok:

Vírusvédelem: ha rossz vírusvizsgálót használunk vagy nem frissítjük, a PC támadhatóvá válik.

Tűzfal: ha egy trójai bejut a PC-be, kijátszhatja a tűzfalat és kiküldheti az adatainkat. Ehhez használhatjuk az *Injection Attack* eljárást, ami „befűz" az Internet Explorerbe egy kódot, amely aztán együtt fut az Explorer.exe-vel, és megmondja neki, hogy mit tegyen. A tűzfal csak a böngészőt ismeri fel, és hagyja tevékenykedni. A károkozónak előbb azonban valahogyan be kellett jutnia, egy CD-vel vagy maillel. Alapve-

tő igazság: a szoftveres tűzfalakat szoftverrel mindig ki is lehet játszani. További példa: egy trójai valamilyen ismert programnak – például *Word-nek* – álcázza magát, és ennek a hamis információnak az alapján korlátlan elérést biztosítunk neki a webre. A károkozónak azonban előzőleg itt is be kellett jutnia valahogy a rendszerbe, például mailben.

Mail: bár az *exe* fájlok blokkolva vannak, a vírusok a *zip* fájlokkal még belopakodhatnak. Az ilyen fájlokat viszont a víruskereső feladata megtalálni.

8 Problémák az XP SP2-vel

Bár az XP Service Pack 2 kétségtelenül jelentős előrelépés a biztonság terén, és remélhetőleg ahhoz is hozzájárul, hogy az internet egészében biztonságosabb „hely" legyen, nem hunyhatjuk be a szemünket a vele kapcsolatos problémák felett sem. Ez a fejezet ezekről a problémákról ad számot.

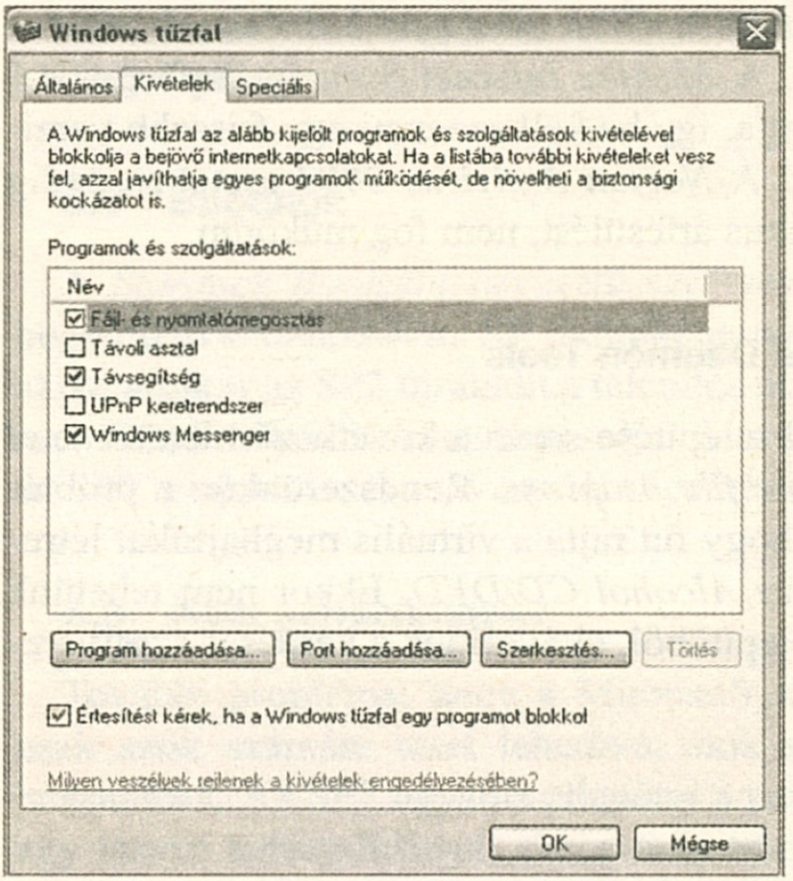
Azzal talán már mindenki tisztában van, hogy számos olyan alkalmazás akad, amely nemigen működik együtt a telepítés után az XP új javítócsomagjával (ezek listáját megtalálhatjuk a webcímen). Bár e problémák általában áthidalhatók a portok saját kezű megnyitásával (ehhez is találunk útmutatót az előbb említett linken), nem várható el a hétköznapi, tapasztalatlanabb felhasználóktól, hogy ezt maguk tegyék meg. Ez persze önmagában sajnos még nem minden: lássuk, az eddig napvilágot látott tapasztalatok alapján milyen problémákkal szembesülhetünk a javítócsomag telepítése után és közben.

8.1 Spyware veszély

A Microsoft figyelmeztette a felhasználókat, hogy irtsák le a spyware-eket a rendszereikről, mielőtt telepítenék az SP2-t. Erre azért van szükség, mert egyes spyware-ek lefagyaszthatják a rendszert a SP2-re frissítés közben. A spyware-ek kiirtása viszonylag könnyedén kivitelezhető olyan ingyenes szoftverekkel, mint az *Ad-aware* vagy a *Spybot SD*.

8.2 XP SP2 webszerverek

Alapértelmezésben a Windows beépített tűzfala blokkolja a forgalmat a legtöbb porton. Ahhoz, hogy lehetővé tegyük a natív és külsős szoftverek futtatását, azonosítanunk kell és meg kell nyitnunk azt a portot vagy portokat, amelyekre ezek az alkalmazások igényt tartanak.



Egyes programok működéséhez „kézzel" kell megnyitnunk a megfelelő port(oka)t

Például amennyiben a webkiszolgálóként konfigurált XP rendszeren a *Frontpage Server Extensionst* vagy a *SharePoint Team Servicest* használjuk, előfordulhat, hogy az IIS által használt portot (80-as TCP port) az alapértelmezésben aktív tűzfal blokkolja. Hogy ezt kiküszöböljük, készítsünk egy szabályt a tűzfalon, amely megnyitja a 80-as portot a bejövő forgalom előtt. Ide kapcsolódik még az is, hogy ha egy FTP segédprogramot használunk egymagában vagy egy alkalmazással karöltve, meg kell nyitnunk a 21-es TCP portot (kapcsolódó információkért lásd: **http://support.microsoft.com/?kbid=883607).**

8.3 Vírusirtó problémák

Az antivírus programok közül jó néhány összeakaszthatja a bajszát a SP2-vel. A problémák számos formában nyilvánulhatnak meg, kezdve azzal, hogy a szoftver nem indul, egészen a rendszer összeomlásáig – bár való igaz, hogy a problémák inkább a régebbi verziókra jellemzőek.

A *McAfee Virusscan Professional 7.0*-nál korábbi verzióinál már a telepítés során akadályba ütközünk *(Webscanx.exe has encountered a problem and needs to close).* A *McAfee Internet Security Software 4.0* ugyanezeket a tüneteket mutatja, így be kell szerezni egy frissebb verziót az SP2 alatti működéshez. A *Norton Antivirus 2003* esetében pedig hiába ütemezünk be automatikus átfésülést, nem fog működni.

8.4 Alcohol CD/DVD és Daemon Tools

Elképzelhető, hogy az SP2 telepítése során a következő hibaüzenetet kapjuk: *Setup cannot copy the file Atapi.sys*. Rendszerünkön a problémát valószínűleg az okozza, hogy fut rajta a virtuális meghajtókat létrehozó a *Daemon Tools* vagy az *Alcohol CD/DVD*. Ekkor nem tehetünk mást, minthogy kilépünk a telepítőből, eltávolítjuk a kérdéses szoftvereket, és újraindítjuk a telepítést.

8.5 UMAX lapolvasók

Ha olyan XP rendszert frissítettünk, ahova előzőleg egy *UMAX* szkenner illesztőprogramját telepítettük, akkor a telepítés befejeztével a rendszer valószínűleg folytonosan újra fog indulni. Hogy ennek véget vessünk, indítsuk újra a gépet *Csökkentett módban hálózattal,* majd távolítsuk el a szóban forgó szkenner illesztőprogramot. Azután – még mindig Csökkentett módban – távolítsuk el az SP2-t úgy, hogy a *Programok hozzáadása/eltávolítását* parancssorból futtatjuk. Ehhez nyissuk meg a parancssort, majd gépeljük be az *appwiz.cpl* sort. Keressük meg a Windows XP SP2-t a programok között, távolítsuk el, majd indítsuk újra a gépet. Feltéve, hogy a szkennerünk nélkül is tudunk élni, most már biztonságosan frissíthetünk SP2-re.

8.6 USB illesztőprogramok

Előfordulhat, hogy az SP2 rosszul jelzi ki az USB illesztőprogramok verziószámát, még akkor is, ha az illesztőprogramokat már lecseréltük újabb verziókkal. Ennek kijavítására indítsuk el az *Eszközkezelőt,* és válasszuk ki az USB-s eszközöket, ahol régebbi verziót jelez a gép, majd válasszuk az *Illesztőprogram frissítése* opciót. Miután az összes USB-s eszköz frissítését elvégeztük, az Eszközkezelőnek már a helyes verziót kell kijeleznie.

8.7 Bootskin

A *Stardock Bootskin* nevezetű szoftverét többen is használják arra, hogy megváltoztassák az XP indítóképernyőjét. Amennyiben a Bootskin aktív, amikor az SP2 újraindít a telepítés után, könnyen kifagyhat a rendszer. Ennek elkerüléséhez kapcsoljuk ki a szoftvert, mielőtt elkezdenénk az SP2 telepítését, és csak ennek végeztével kapcsoljuk vissza.

8.8 Nem mindenkinek?

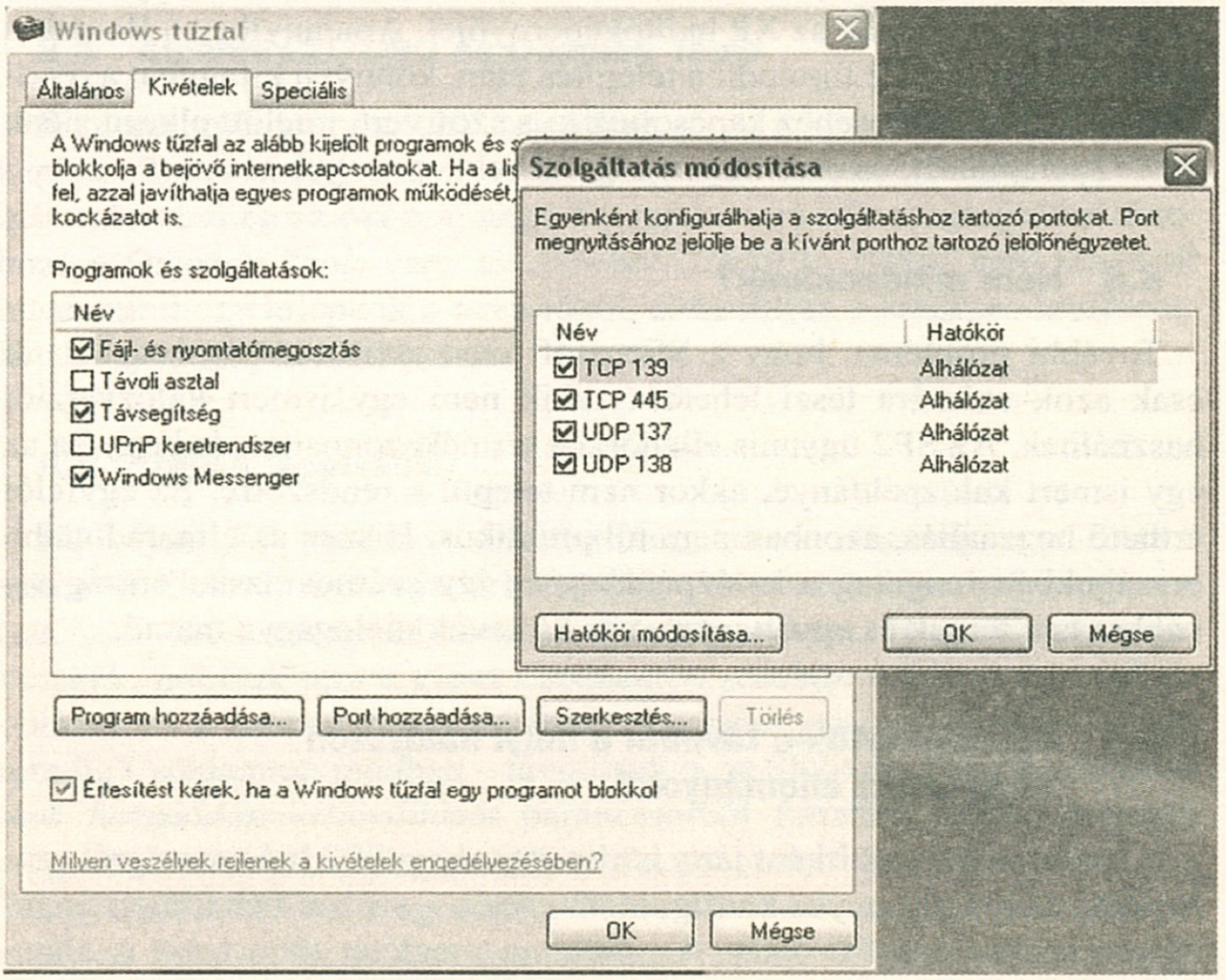
További probléma, hogy a Microsoft eme javítócsomag használatát csak azok számára teszi lehetővé, akik nem egy ismert kalózverziót használnak. Az SP2 ugyanis ellenőrzi a termékazonosítót, és hogy ha az egy ismert kalózpéldányé, akkor nem települ a rendszerre. Ez egyfelől érthető hozzáállás, azonban nem túl praktikus. Hiszen az elmaradottabb országokban rengeteg a kalózpéldány, és így számos ázsiai ország továbbra is a férgek és egyéb internetes kártevők melegágya marad.

8.9 Hozzáférhetők-e távolról a helyi hálózaton megosztott állományok?

Az internetet rémhírként járta körbe egy olyan SP2 hiányosságról szóló cikk, mely – bizonyos konfiguráció esetén – szabad betekintést engedélyez bárkinek a PC-nken. A probléma meglétét több teszt is alátámasztotta. Miről van pontosan szó? Amikor telepítjük az SP2-t, a meg-

osztott fájlok és nyomtatók bárki számára szabadon megtekinthetők – az aktivált tűzfal ellenére. Csupán annyi kell ehhez, hogy az elemek meg legyenek osztva a belső hálózaton. A modemes és ISDN-nel kapcsolódók teljes mértékben ki vannak szolgáltatva ennek a hibának, míg a DSL szolgáltatást használók csak akkor, ha nincs integrált tűzfal a modemükben, illetve ha nem DSL routert használnak. Továbbá az internetkapcsolat-megosztásnak (ICS) kikapcsolva kell lennie.

Tehát a probléma elég gyakori. Aki egy kis energiát fektet a dologba, hamarosan könnyen elérhető gépekbe botlik az interneten, amelyek esetében a felhasználók abban a hiszemben élnek, hogy megosztott állományaik csak a helyi hálózaton lévő gépek számára láthatók. Gyakran még csak jelszavas védelemmel sem találkozunk.



Ne tegyük ki megosztott állományainkat a világ szeme elé!

A problémát az okozza, hogy az SP2 elővigyázatlanul átveszi a tűzfal korábbi beállításait: amennyiben az aktív volt a betárcsázós kapcsolatnál, a hálózati adapternél is aktiválva lesz. Ugyanakkor a kivételek közé kerül a fájl és nyomtatómegosztás a belső hálózati kártyánál és az összes adapter esetében. A SP2 feltelepülése után a betárcsázós kapcsolat használatakor minden megosztott adatunk láthatóvá válik a neten. A probléma szerencsére orvosolható. A *Vezérlőpulton* válasszuk a *Windows tűzfalat,* majd a *Kivételek* fület. Itt kattintsunk a *Fájl- és nyomtatómegosztásra,* majd a *Szerkesztés* gombra. Ekkor láthatjuk a négy portot, amelyet a Fájl- és nyomtatómegosztás használ. Ahhoz, hogy a szolgáltatást csak a belső LAN-ra korlátozzuk, válasszuk ki a megfelelő „hatókört".

8.10 Konklúzió

Szeretnénk jelezni, hogy a fentebb ismertetett problémák valószínűleg pusztán csak töredékét képezik annak, ami napvilágra fog kerülni a közeljövőben, ahogy egyre több és több felhasználó telepíti az SP2-t a világ minden táján. Mindenesetre ez ne tartson vissza minket a telepítéstől, hiszen egy valóban hasznos védelmi javítás kerül a gépünkre, ami főleg azért értékes, mert felhasználók millióit fogja rávezetni a biztonságosabb Windows környezet kialakítására. Azzal ugyanis, hogy a tűzfal, az antivírus és a Windows frissítése általánossá válik, az egyéni felhasználókon kívül az internet teljes közössége is sokat nyer.

9 A 2. szervizcsomag üzleti értéke

A Microsoft Windows XP továbbfejlesztett biztonsági technológiákat tartalmazó 2. szervizcsomagja bővített biztonsági infrastruktúrát kínál a vírusok, férgek és behatolók elleni hatékony védekezéshez. Hatékonyabb eszközöket nyújt az informatikai szakemberek számára a biztonsági szolgáltatások kezeléséhez és felügyeletéhez, a

felhasználók számára pedig kényelmesebb használatot biztosít. Ez a fejezet azt ismerteti, hogy a Windows XP alapú számítógépeken miként tehető hatékonyabbá és könnyebbé a vállalati adatok védelme és a biztonsági szolgáltatások kezelése, és miként biztosítható a felhasználók produktivitása a 2. szervizcsomag telepítésével.

9.1 Áttekintés

Szinte minden számítógépeket használó szervezet rendelkezik olyan adatokkal, amelyek védelméről gondoskodni kell. Ezek közé tartoznak például az értékesítési tippek, a termékfejlesztési tervek, az alkalmazottak adatai stb. A szigorú szabályozási feltételek között működő nyilvános részvénytársaságoknak, pénzügyi intézményeknek és egészségügyi szervezeteknek is fokozott védelemben kell részesíteniük számítógépeiket a bizalmas adatok (pénzügyi kimutatások, betegek adatai stb.) megszerzésére irányuló támadásokkal szemben.

Furcsa módon a legtöbb támadás azokat az ismert sebezhető pontokat éri, amelyek egyébként a rendelkezésre álló óvintézkedések betartásával megvédhetők lennének. Az óvintézkedések közé sorolhatók az operációs rendszerek már meglévő szolgáltatásai – például a tűzfalak, illetve az e-mail mellékletekkel és a makrókkal kapcsolatos biztonsági funkciók – és a szoftverfrissítések. Bár e megelőző eszközök rendelkezésre állnak, a Microsoft tisztában van azzal is, hogy a felhasználók egyre nehezebben tudnak lépést tartani azokkal az egyre-másra megjelenő szoftverfrissítésekkel, amelyek a számítógépeik elleni támadások elhárításához szükségesek.

Ezért a Microsoft folyamatosan törekszik arra, hogy termékei már eleve biztonságosabbak legyenek. A *Microsoft Windows Server 2003* és a *Microsoft Office 2003* különböző változatai már valódi sikerekkel büszkélkedhetnek e téren. Ez a kezdeményezés tovább folytatódik a *Windows XP 2. szervizcsomagjának* kiadásával is. A Microsoft célja, hogy a lehető legrugalmasabb és legbiztonságosabb szoftvert bocsássa a felhasználók rendelkezésére. A vállalat elkötelezte magát amellett, hogy

a támadásokkal szemben ellenállóképesebb rendszereket hozzon létre még olyan esetekre is, amikor nem elérhetők a frissítések, vagy nem telepíthetők azonnal.

A Windows XP 2. szervizcsomagja gyors és ingyenes lehetőséget kínál a vállalatoknál működtetett Windows XP alapú számítógépek védelmének megerősítésére a Microsoft továbbfejlesztett biztonsági technológiái és újításai révén. A megerősített biztonsági infrastruktúra megkönnyíti a vírusok, hackerek és férgek elleni védekezést, a kezelhetőséget és az ellenőrzést lehetővé tevő eszközök segítségével pedig egyidejűleg biztosítható a kényelem és a biztonság is. A szervizcsomag segítségével növelhető a felhasználói hatékonyság is azáltal, hogy elkerülhetők a nagy időveszteséget okozó támadások.

9.2 A hálózati infrastruktúra megerősítése

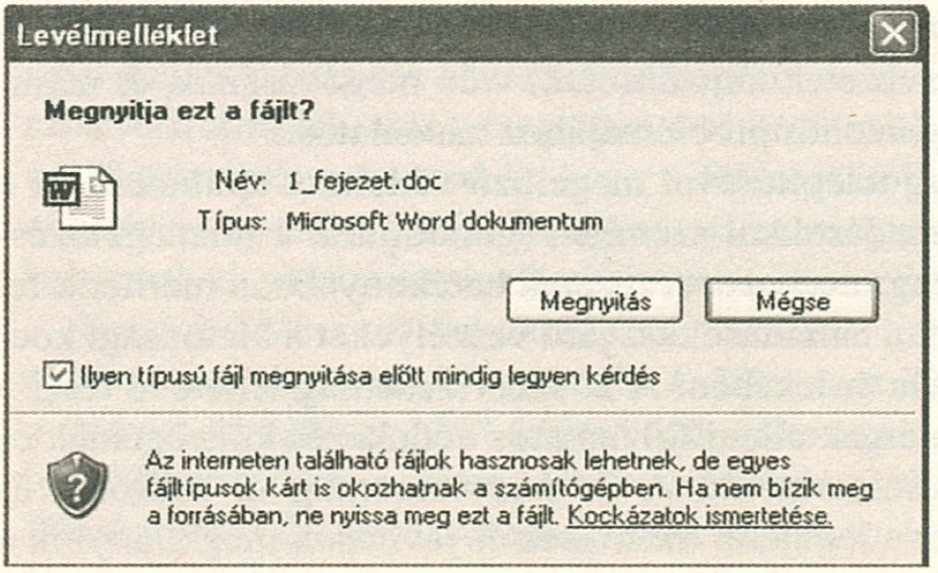
Manapság a biztonság jelenti a legnagyobb informatikával kapcsolatos kihívást a szervezetek számára. Szinte minden szervezetnek vannak már tapasztalatai az utóbbi időkben elterjedt vírusokkal, köztük a *Blaster*, a *Mydoom* és a *Sasser* vírussal. A vírussal fertőzött számítógépek megtisztítása és a vírusokkal szembeni védettség kialakítása bonyolult, fárasztó és költséges feladat. Ezt az eljárást nagyrészt manuálisan kell elvégezni, az informatikai részleg teljes bevonásával, különösen a nagyobb szervezeteknél. A fertőzött számítógépek utólagos megtisztítása nem a leghatékonyabb módja a szervezetek támadásoktól való megóvásának, és némiképp a tűzmegelőzés–tűzoltás problémájához hasonlatos.

A 2. szervizcsomag telepítésével megelőző védelmet építhetünk ki a számítógépeken a támadásokkal szemben (gondoljunk a tűzmegelőzésre). A 2. szervizcsomag révén a szervezetek hatékonyabban mérhetik fel előre és mérsékelhetik a támadásokkal járó veszélyeket a biztonsági kockázatok minimalizálása érdekében. A 2. szervizcsomag lehetővé teszi a hackerek, vírusok és férgek elleni folyamatos védekezés költségeinek és kudarcélményeinek csökkentését. A 2. szervizcsomag új eszközei és technológiái, valamint a legújabb frissítések és javítások megkönnyítik a vállalatok számára a biztonság fokozását és a létfontosságú üzleti erőforrások hatékonyabb védelmét.

A biztonsági infrastruktúra megerősítésével a 2. szervizcsomag ellenállóbbá teszi a szervezetek számítógépeit és az azokon tárolt adatokat a támadásokkal szemben. Gyakran előfordul, hogy a biztonsági frissítéseket nem telepítik, vagy nem lehet telepíteni rögtön a kibocsátásukat követően, de ez esetben is védelemre van szükség az ugyanolyan típusú fenyegetésekkel szemben, mint amelyek ellen a biztonsági frissítéseket létrehozták. A 2. szervizcsomag olyan biztonsági technológiát tartalmaz, amely fokozott védelmet nyújt abban az esetben is, ha a biztonsági frissítéseket nem telepítik azonnal.

A 2. szervizcsomag a következő előnyöket biztosítja a szervezetek hálózati infrastruktúrája számára:

A hálózat megvédése a hálózati támadásoktól. A Windows tűzfal erősebb védelmet nyújt a hálózati támadásokkal szemben azáltal, hogy blokkolja a kéretlen bejövő forgalmat. A 2. szervizcsomag által biztosított továbbfejlesztett tűzfal a rendszer indításakor és leállításakor is fokozottan védi a számítógépet. A 2. szervizcsomag alapértelmezés szerint bekapcsolja a Windows tűzfalat arra az esetre, ha a felhasználó a kezdeti konfigurálás során erről elfeledkezne. E szolgáltatás segítségével számos pusztító támadást lehet megelőzni még akkor is, ha a szoftverfrissítések nem telepíthetők azonnal. Telepített 2. szervizcsomag és bekapcsolt Windows tűzfal esetén a 2003-ban elterjedt Blaster féreg sokkal kevesebb kárt oko-



A mellékletek megnyitásakor a Outlook Express szeparálja a potenciálisan veszélyes csatolmányokat

zott volna a szervezeteknek. Ennek a féregnek a terjedéshez szabad hozzáférésre van szüksége a számítógépek portjaihoz. A Windows tűzfal véletlenszerű beállítása helyett a 2. szervizcsomag a beállítások teljes körű és rugalmas ellenőrzését kínálja a szervezetek számára.

A hálózat megvédése az e-mailek, azonnali üzenetek és weblapok segítségével terjedő vírusokkal szemben. Az e-mail gyakori hordozója és terjesztője a számítógépeket megfertőző vírusoknak. Amikor egy vírus megkezdi akadálytalan tovaterjedését, megbénítja az e-mail kiszolgálókat, csökkenti a levelezés hatékonyságát, és az eltávolítása nagy költségeket emészt fel. A 2. szervizcsomag olyan új szolgáltatásokat tartalmaz, amelyek biztonságosabbá teszik a *Microsoft Outlook Express,* a *Microsoft Outlook,* a *Windows Messenger* és a *Microsoft Internet Explorer* használatát azáltal, hogy megakadályozzák a *Sobig.F*-hez hasonló vírusok elterjedését. A mellékletek megnyitásakor például a *Mellékletkezelő* elkülöníti a Windows által nem biztonságosnak ítélt mellékleteket. Ezzel nagy mértékben csökkenthető a vírusok okozta károk valószínűsége.

A 2. szervizcsomag tartalmazza továbbá a mellékletek végrehajtását kezelő *Attachment Execution Services (AES)* nyilvános API-felületet, melynek segítségével a fejlesztők egységes és biztonságos mellékletkezelést építhetnek be alkalmazásaikba.

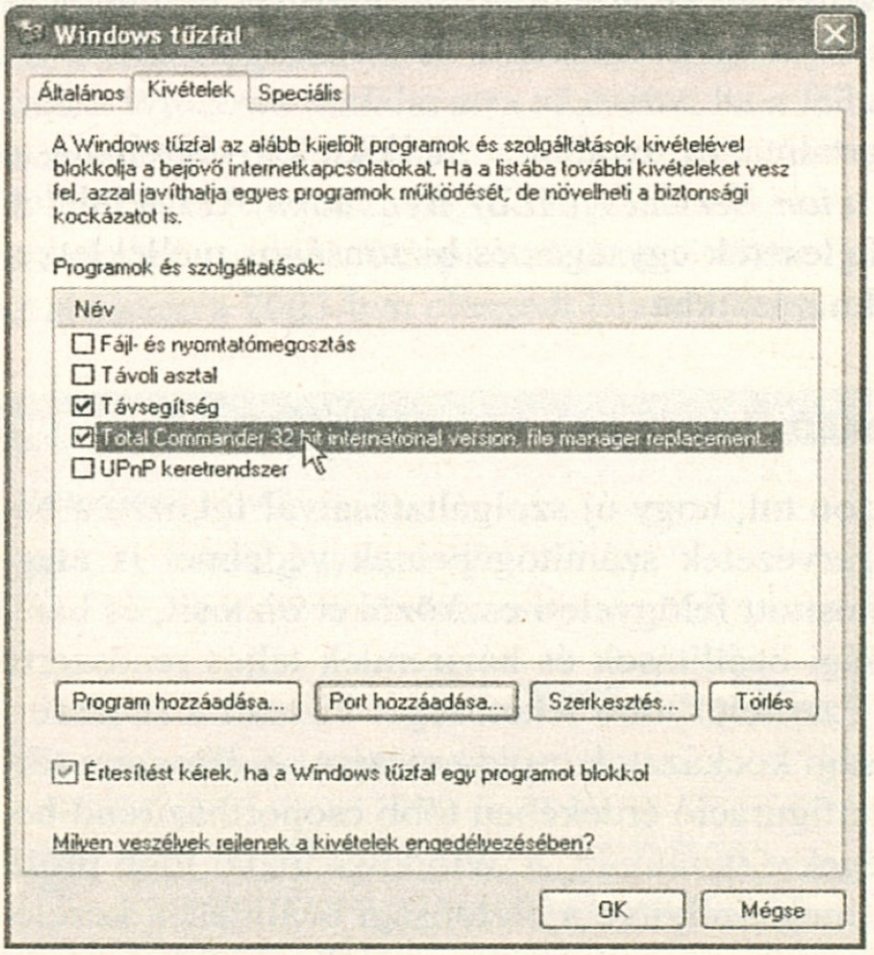
9.3 A hálózati biztonság kezelése és szabályozása

A 2. szervizcsomag azon túl, hogy új szolgáltatásaival fokozza a hálózatok biztonságát, a szervezetek számítógépeinek védelmét is megkönnyíti. Jobban központosított felügyeleti eszközöket biztosít, és hatékonyabbá teszi a biztonsági beállítások és házirendek teljes rendszerre kiterjedő szabályozását. Ezenfelül több lehetőséget biztosít a rendszergazdák számára a biztonsági kockázatok csökkentésére. A *Windows tűzfal* például a rugalmas konfiguráció érdekében több csoportházirend-beállítást és egyéb lehetőségeket tartalmaz. A Windows tűzfal több profil használatát is támogatja, megkönnyítve a biztonsági beállítások kezelését azokban az esetekben, amikor a mobil felhasználók többféle kapcsolattal rendelkeznek.

A 2. szervizcsomag a hálózatbiztonság szabályozásához a következő lehetőségeket biztosítja a rendszergazdák számára:

A biztonsági beállítások központi kezelése. A 2. szervizcsomag a korábbinál több beállítási lehetőséget biztosít a rendszergazdák számára, beleértve a csoportházirendet, a parancssorból történő konfigurálást, a csoportos címzés támogatását és a felügyelet nélküli telepítést. A Windows tűzfal központi kezelése – az esetleges biztonsági beállítások helyett – biztosítja a szervezetek informatikai részlege számára az összes számítógép konfigurálásához szükséges központi szabályozást az elérhető leghatékonyabb megelőző védelem kialakítása érdekében.

Gyors reagálás a támadásokra. A Windows tűzfal központi kezelése lehetővé teszi az informatikai részlegek számára, hogy gyorsabban reagáljanak a biztonságra veszélyes fenyegetésekre. E szolgáltatás segítségével a rendszergazdák, észlelve a támadásokat, gyorsan és központilag



A Windows tűzfal kivétellistájával lehetővé válik, hogy csak egy-egy biztonságos alkalmazás bonyolíthasson webforgalmat

módosíthatják a biztonsági beállításokat. Gyorsan lezárhatják például a portokat egy új féreg támadására reagálva.

A többféle hálózati környezetben dolgozó felhasználók támogatása. A többféle tűzfalprofil használatának csoportházirenden keresztüli támogatása lehetővé teszi, hogy a rendszergazdák más és más konfigurációt állítsanak be arra az esetre, amikor a felhasználók a vállalati hálózathoz csatlakoznak, és arra az esetre, amikor utaznak. Az alternatív tűzfalprofilok rugalmassága nagyobb biztonságot jelent a vállalat összes mobil felhasználója számára. Az informatikai szakemberek például úgy konfigurálhatják a mobil felhasználók vállalati hálózati kapcsolatának tűzfalát, hogy azok használhassák a szükséges alkalmazásokat, de a telefonos kapcsolatukat eltérő tűzfalbeállításokkal lehet konfigurálni annak érdekében, hogy számítógépük fokozottan védve legyen a vállalati tűzfalon kívül.

A tűzfal konfigurálása az alkalmazások kompatibilitásának biztosítására. A Windows tűzfal kivétellistája lehetővé teszi, hogy a rendszergazdák biztonságosabban kezelhessék az alkalmazásokat azáltal, hogy csak az adott alkalmazás számára szükséges portokat nyitják meg.

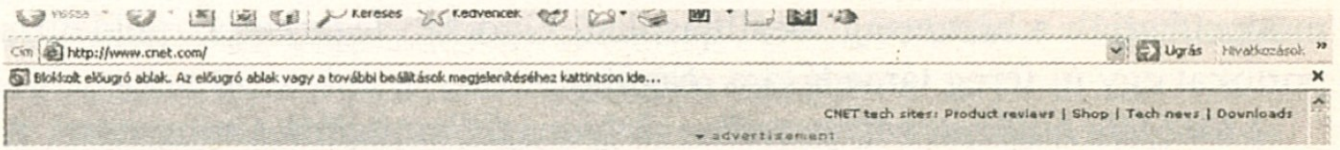
Ezzel a szolgáltatással biztosítható, hogy az informatikai részleg úgy telepíthesse és konfigurálhassa a tűzfalat, hogy közben az alkalmazások továbbra is megfelelően működjenek. A biztonság további növelése érdekében a rendszergazda beállíthatja, hogy az alkalmazások csak a helyi hálózatról fogadhatnak forgalmat, az internetről azonban nem.

9.4 Nagyobb biztonság a felhasználók számára

A Windows XP 2. szervizcsomagja új szolgáltatásokat tartalmaz az e-mail és az azonnali üzenetküldés biztonságosabbá tételéhez. Olyan új beépített eszközöket is magában foglal – például az előugró ablakok blokkolását –, amelyek megkönnyítik a számítógép-használat biztonságosabbá és hatékonyabbá tételét.

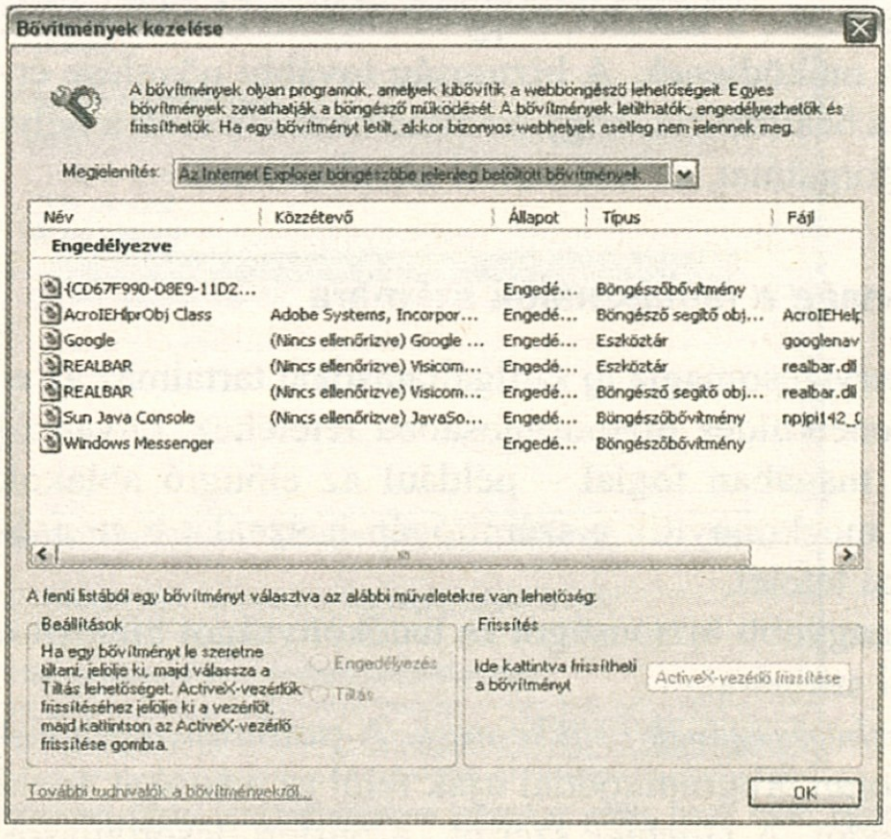
A 2. szervizcsomag nagyobb biztonságot és hatékonyságot biztosít a szervezetek felhasználói számára:

A számítógépek sebezhetőségének csökkentése. A puffertúlcsordulást kihasználó támadások során programkóddal írják felül az adatokat, majd futtatják a bejuttatott kódot. A *Gartner* szerint „a puffertúlcsordulások



Az előugró ablakok blokkolásáról az úgynevezett információs sáv tájékoztat

gyakori célpontjai lettek a támadásoknak, és a legelterjedtebb fertőzések közül néhány, így az MSBlast, a Slammer és a Nimda számára biztosítottak szabad utat." A 2. szervizcsomag a puffertúlcsordulást kihasználó támadások egy komplett típusát elhárítja azáltal, hogy a processzorszolgáltatások segítségével csak azokon a memóriaterületeken engedélyezi programkód végrehajtását, amelyek kifejezetten végrehajthatóként vannak megjelölve (a szolgáltatáshoz NX-kompatibilis processzor szükséges). Az Internet Explorer programkód szintű módosítása sok más sebezhető pont elleni támadást akadályoz meg. A *Helyi számítógép* zóna zárolásával például megakadályozható, hogy a hackerek úgy támadjanak meg számítógépeket, hogy HTML kódot futtatnak a Helyi számítógép zónában kiemelt rendszerfelhasználói jogosultságokkal.



Az SP2-vel könnyen ellenőrzésünk alatt tarthatjuk az Internet Explorer bővítményeit

A felhasználók megóvása az előugró hirdetésektől és a megtévesztő fájlkiterjesztésektől (spoofing). Az előugró ablakok a weblapok kéretlen hirdetéseit és tartalmát jelenítik meg automatikusan a felhasználók számítógépén. Sok bosszúságot okoznak a felhasználóknak, és csökkentik az internetes munkavégzés hatékonyságát. A 2. szervizcsomag új, beépített szolgáltatást kínál az előugró ablakok blokkolására, melynek segítségével csökkenthető a kéretlenül megjelenő hirdetések száma.

A 2. szervizcsomag Internet Explorert érintő egyik javítása a megtévesztő felhasználói felület megjelenítésével a személyes adatokhoz való illetéktelen hozzáférés *(phishing)* megakadályozását célozza meg. Az Internet Explorer megnehezíti a webhelyek számára a párbeszédpanelekre hasonlító olyan böngészőablakok megjelenítését, amelyek kéretlenül egy programot telepítenek, miután a felhasználó a *Cancel* (Mégse) gombra kattint az ablak bezárásához.

A kéretlen programok véletlenül történő letöltésének és futtatásának megakadályozása. A 2. szervizcsomag védelmet nyújt a potenciálisan kártékony webhelyekről származó programok nem szándékos letöltése és telepítése ellen a letöltési kérelmek automatikus blokkolásával, védve ezzel a felhasználót. Azok, akik a program telepítését választják, a böngésző eszköztára alatt automatikusan megjelenő letöltési hivatkozásra kattintva ezt megtehetik. A szervezetek informatikai részlegei ezt a szolgáltatást a meglévő eszközök, például a *Microsoft Active Directory* címtárszolgáltatás csoportházirendje segítségével felügyelhetik. Az Internet Explorer új biztonsági technológiái kiegészítik a webtartalom szűrésére már létező megoldásokat, fokozott védelmet nyújtva a vállalati és a hordozható számítógépek számára.

9.5 Javaslatok

A Windows XP 2. szervizcsomagja megkönnyíti a biztonsági fenyegetések kockázatának csökkentését azáltal, hogy megerősíti a hálózat védelmét, a magas szintű biztonságot alapértelmezés szerint beállítja, és lehetővé teszi a rendszergazdák számára, hogy hatékonyabban kezelhessék a biztonsági beállításokat és házirendeket. Ezen előnyök ellenére az alkalmazások kompatibilitása a legtöbb szervezet számára továbbra is

kényes kérdés marad. A Gartner szerint: „Bár a kereskedelmi forgalomban kapható dobozos szoftverek kevesebb mint 3 százaléka, az egyéni alkalmazásoknak pedig kevesebb mint 5 százaléka ütközik a 2. szervizcsomaggal (70%-os valószínűséggel), a vállalatok legalább 30 százalékánál lesz legalább egy alkalmazás, amely nem kompatibilis a 2. szervizcsomaggal (70%-os valószínűséggel)."

A Microsoft és partnerei gondosan tesztelik az alkalmazásokat, és megoldásokat kínálnak e problémákra. „Azáltal, hogy a rosszindulatú támadásokat főként a belépési pontnál blokkolja, a Windows XP 2. szervizcsomagja jelentős lépésnek számít ügyfeleink számítógépes infrastruktúrájának hatékony megvédésében" – mondta *Tom Button,* a Windows ügyfélmarketing részlegének alelnöke. „Ugyanakkor jelentős összegeket fordítunk a telepítéssel és az alkalmazások kompatibilitásával kapcsolatos problémák minimalizálására annak érdekében, hogy ügyfeleink teljes mértékben kihasználhassák a Windows XP 2. szervizcsomagja nyújtotta előnyöket."

Az a tény, hogy a 2. szervizcsomag ütközhet néhány alkalmazással, nem késleltetheti a szervizcsomag kiértékelését a szervezeteknél. A *Forrester Research* azt ajánlja minden Windows XP felhasználónak, hogy amint lehet, frissítse rendszerét a 2. szervizcsomaggal. Fontos, hogy először a szervezet által használt alkalmazásokat kell alaposan tesztelni. A Gartner szerint: „Mint minden szervizcsomag vagy egyéb jelentős módosítás esetében, a vállalatoknak a 2. szervizcsomag esetében is a lehető legtöbb alkalmazásnál kell kompatibilitási tesztet végezniük. Ha mindet nem lehet, akkor azokat az alkalmazásokat kell tesztelni, amelyeket a legtöbb felhasználó használ, és amelyek létfontosságúak a vállalat számára."

9 789632 170916
Ára: 990 Ft

Microsoft

A gördülékenyebb munka ára:

61 900 Ft*

© 2004 Microsoft Corporation. Minden jog fenntartva.
A Microsoft és az Office Small Business Edition 2003 logó a Microsoft Corporation bejegyzett védjegye vagy védjegyei az Egyesült Államokban és/vagy más országokban.

Az Ön vállalkozásának bizonyára egy célja van: az üzleti siker. Ebben segít most a Microsoft Office 2003 Small Business Edition. Gördülékennyé és egyszerűvé teszi a partnerekkel történő kommunikációt, az ügyfelek kezelését és nyilvántartását, illetve professzionális marketinganyagok és prezentációk elkészítését mind Önnek, mind alkalmazottainak. Minden nap.
Bővebb információ: www.microsoft.com/hun/officesbe weboldalon vagy hívja a 2 MSINFO (267-4636) telefonszámot.

Microsoft Office Word 2003
Microsoft Office Excel 2003
Microsoft Office Outlook 2003 with Business Contact Manager
Microsoft Office Publisher 2003
Microsoft Office PowerPoint 2003

Most PC vásárlása nélkül is kedvező áron!

Microsoft Office
Small Business Edition 2003

* Javasolt nettó végfelhasználói ár. Az ajánlat a készlet erejéig tart, és a dobozos, magyar nyelvű verzióra vonatkozik.